

DECIDING CONDITIONAL TERMINATION

MARIUS BOZGA, RADU IOSIF, AND FILIP KONEČNÝ

VERIMAG, CNRS, 2 av. de Vignate, 38610 Gières, France
e-mail address: bozga@imag.fr

VERIMAG, CNRS, 2 av. de Vignate, 38610 Gières, France
e-mail address: iosif@imag.fr

VERIMAG, CNRS, 2 av. de Vignate, 38610 Gières, France
e-mail address: konecny@imag.fr

ABSTRACT. We address the problem of conditional termination, which is that of defining the set of initial configurations from which a given program always terminates. First we define the dual set, of initial configurations from which a non-terminating execution exists, as the greatest fixpoint of the function that maps a set of states into its pre-image with respect to the transition relation. This definition allows to compute the non-termination precondition if either (i) the transition relation is deterministic, (ii) the descending Kleene sequence overapproximating the greatest fixpoint converges in finitely many steps, or (iii) the transition relation is well-founded. We show that this is the case for two classes of relations, namely octagonal and finite monoid affine relations. Moreover, since the closed forms of these relations can be defined in Presburger arithmetic, we obtain the decidability of the termination problem for such loops.

We show that the weakest non-termination precondition for octagonal relations can be computed in time polynomial in the number of variables of the relation. Furthermore, for every well-founded octagonal relation, we prove the existence of an effectively computable well-founded witness relation for which a linear ranking function exists.

For the class of linear affine relations we show that the weakest non-termination precondition can be defined in Presburger arithmetic if the relation has the finite monoid property. Otherwise, for a more general subclass, called polynomially bounded affine relations, we give a method of under-approximating the termination preconditions.

Finally, we apply the method of computing weakest non-termination preconditions to more complex transition relations, by relying on the computation of transition invariants. In this way we could infer non-termination preconditions of several programs. These preliminary experiments provided encouraging results, reported in this paper.

1998 ACM Subject Classification: D.2.8 – Software Engineering – Software/Program Verification – formal methods, model checking .

Key words and phrases: Integer Programs, Periodic Relations, Recurrent Sets, Termination Preconditions.

This work was supported by the Czech Science Foundation (projects P103/10/0306, 102/09/H042, 201/09/P531), the Czech Ministry of Education (project COST OC10009, Czech-French Barrande project MEB021023, the long-term institutional project MSM0021630528), the European Science Foundation (ESF COST action IC0901), the EU/Czech IT4Innovations Centre of Excellence (project ED1.1.00/02.0070), the French National Research Agency (project ANR-09-SEGI-016 VERIDYC), and the Brno University of Technology (projects FIT-S-10-1, FIT-S-11-1, FIT-S-12-1).

1. INTRODUCTION

The termination problem asks whether every computation of a given program ends in a halting state. The universal termination asks whether a given program stops for every possible input configuration. Both problems are among the first ever to be shown undecidable, by A. Turing [34]. In many cases however, programs will terminate when started in certain configurations, and may¹ run forever, when started in other configurations. The problem of determining the set of configurations from which a program terminates on all paths is called *conditional termination*.

In program analysis, the presence of non-terminating runs has been traditionally considered faulty. However, more recently, with the advent of *reactive systems* [25], accidental termination can be an equally serious error. For instance, when designing a web server, a developer would like to make sure that the main program loop will not exit unless a stopping request has been issued. These facts led us to considering the *conditional non-termination* problem, which is determining the set of initial configurations which guarantee that the program will not exit.

In this paper we focus on programs that handle integer variables, performing Presburger arithmetic tests and (possibly non-deterministic) updates. A first observation is that the set of configurations guaranteeing non-termination is the greatest fixpoint of the pre-image pre_R of the program's transition relation² R . This set, called the *weakest recurrent set*, and denoted $wrs(R)$ in our paper, can be computed if either (i) the pre-image of the transition relation is continuous (this is the case, for instance, when the transition relation is deterministic), (ii) the descending Kleene sequence that overapproximates the greatest fixpoint eventually stabilizes, or (iii) the relation is well-founded and $wrs(R) = \emptyset$. If one of these conditions holds and moreover, the closed form of the infinite sequence of relations $\{R^i\}_{i \geq 0}$, obtained by composing the transition relation with itself 0, 1, 2, ... times, can be defined using a decidable fragment of arithmetic, we obtain decidability proofs for the universal termination problem, for free.

Contributions of this paper. The main novelty in this paper is of rather theoretical nature: we show that the non-termination preconditions for integer transition relations defined as either *octagons* or *linear affine loops with finite monoid property* are definable in quantifier-free Presburger arithmetic. Thus, the universal termination problem for such program loops is decidable. However, since quantifier elimination in Presburger arithmetic is a complex procedure, we have developed alternative ways of deriving the preconditions for non-termination, and in particular:

- for *octagonal relations*, we use a result from [8], namely that the sequence $\{R^i\}_{i \geq 0}$ is, in some sense, periodic. Based on this, we develop an algorithm that computes the weakest non-termination precondition of R in time polynomial in the number of variables of R . Moreover, we investigate the existence of linear ranking functions and prove that for each well-founded octagonal relation, there exists an effectively computable witness relation, i.e., a well-founded relation that has a linear ranking function.

¹If the program is non-deterministic, the existence of a single infinite run, among other finite runs, suffices to consider an initial configuration non-terminating.

²This definition is the dual of the *reachability set*, needed for checking safety properties: the reachability set is the least fixpoint of the post-image of the transition relation.

- for *linear affine relations*, weakest recurrent sets can be defined in Presburger arithmetic if we consider several restrictions concerning the transformation matrix. If the matrix A defining R has eigenvalues which are either zeros or roots of unity, all non-zero eigenvalues being of multiplicity one (these conditions are equivalent to the finite monoid property of [5, 18]), then $wrs(R)$ is Presburger definable. Otherwise, if all non-zero eigenvalues of A are roots of unity, of multiplicities greater or equal to one, $wrs(R)$ can be expressed using polynomial terms. In this case, we can systematically issue Presburger termination preconditions.

Practical applications. Unfortunately, in practice, the cases in which the closed form of the sequence $\{R^i\}_{i \geq 0}$ is definable in a decidable fragment of arithmetic, are fairly rare. All relations considered so far are conjunctive, meaning that they can represent only simple program loops of the form `while(condition){body}` where the loop body contains no further conditional constructs. In order to deal with more complicated program loops, we use the method of *transition invariants* [28] to compute (sound overapproximations of) weakest non-termination preconditions for programs with complex transition relations. Concretely, we compute an overapproximation of the transition invariant, which is the transitive closure of the transition relation, i.e. R^+ , restricted to the states reachable from some set of initial configurations. If one can find a finite union $R_1^\# \cup \dots \cup R_m^\#$ of octagonal relations that overapproximates the transition invariant, then $wrs(R_1^\#) \cup \dots \cup wrs(R_m^\#)$ is an overapproximation of the weakest non-termination set of R .

This method can infer non-termination preconditions for programs without procedure calls. It is moreover shown to be complete for a class of programs without nested loops, called *flat programs*. On what concerns programs with (recursive) calls, one can compute (overapproximations of) the summaries of the procedures in the program and use these summaries to generate a program without calls that has an equivalent weakest non-termination precondition, following the method described in [3]. We have implemented the computation of transition invariants and procedure summaries in the FLATA tool for the analysis of integer programs. Several experiments on inferring (non-)termination preconditions have been performed, and reported.

Roadmap. The paper is organized as follows. Section 2 introduces the notation and some basic concepts needed throughout the paper. Section 3 defines weakest recurrent sets as greatest fixpoints of the pre-image of the transition relation. Sections 4 and 5 apply this definition to the computation of weakest recurrent sets for octagonal and linear affine relations. Section 6 extends the computation of weakest termination preconditions from simple conjunctive loops to integer programs, and Section 7 reports on the implementation and experiments performed on several integer programs. Finally, Section 8 concludes.

The core results presented in this paper have been reported in [9]. In addition to the work presented in [9], here we improve the time complexity for the computation of weakest non-termination preconditions for octagonal relations, and give a polynomial time algorithm. Moreover, we extend the results from [9] from simple conjunctive program loops to computing non-termination preconditions for full integer programs, and give a decidability result to the universal termination problem, for a class of programs without nested loops.

1.1. Related Work. The literature on program termination is vast. Most work focuses however on universal termination, such as the techniques for synthesizing linear ranking functions of Sohn and Van Gelder [32] or Podelski and Rybalchenko [27], and the more sophisticated method of Bradley, Manna and Sipma [12], which synthesizes lexicographic polynomial ranking functions, suitable when dealing with disjunctive loops. However, not every terminating program (loop) has a linear (polynomial) ranking function. In this paper, we show that for an entire class of non-deterministic linear relations, defined using octagons, termination is always witnessed by a computable octagonal relation that has a linear ranking function.

Another line of work considers the decidability of termination for simple (conjunctive) linear loops. Initially, Tiwari [33] showed decidability of termination for affine linear loops interpreted over *reals*, while Braverman [13] refined this result by showing decidability over *rationals* and over *integers*, for homogeneous relations of the form $C_1\mathbf{x} > 0 \wedge C_2\mathbf{x} \geq 0 \wedge \mathbf{x}' = A\mathbf{x}$. The non-homogeneous integer case seems to be much more difficult as it is closely related to the open *Skolem's Problem* [20]: given a linear recurrence $\{u_i\}_{i \geq 0}$, determine whether $u_i = 0$ for some $i \geq 0$.

To our knowledge, the first work on proving non-termination of simple loops is reported in [19]. The notion of *recurrent sets* occurs in this work, however, without the connection with fixpoint theory, which is introduced in the present work. Finding recurrent sets in [19] is complete with respect to a predefined set of templates, typically linear systems of rational inequalities.

The work which is closest to ours is probably that of Cook et al. [15]. In that paper, the authors develop an algorithm for deriving termination preconditions by first guessing a ranking function candidate (typically the linear term from the loop condition) and then inferring a supporting assertion which guarantees that the candidate function decreases with each iteration. The step of finding a supporting assertion requires a fixpoint iteration in order to find an invariant condition. Unlike our work, the authors of [15] do not address issues related to completeness: the method is not guaranteed to find the weakest precondition for termination, even in cases when this set can be computed. On the other hand, it is applicable to a large range of programs extracted from real-life software. To compare our method with theirs, we tried the examples available in [15]. For those which are polynomially bounded affine relations, we used our under-approximation method and have computed termination preconditions, which turn out to be slightly more general than the ones reported in [15].

2. PRELIMINARY DEFINITIONS

We denote by \mathbb{Z} , \mathbb{N} and \mathbb{N}_+ the sets of integers, positive (including zero) and strictly positive integers, respectively. We denote by \mathbb{Z}_∞ and $\mathbb{Z}_{-\infty}$ the sets $\mathbb{Z} \cup \{\infty\}$ and $\mathbb{Z} \cup \{-\infty\}$, respectively. In this paper we use a set of variables $\mathbf{x} = \{x_1, x_2, \dots, x_n\}$, for some $n > 0$. The set of *primed* variables is $\mathbf{x}' = \{x'_1, x'_2, \dots, x'_n\}$. These variables are assumed to be ranging over \mathbb{Z} . For a set $S \subseteq \mathbb{Z}$ of integers, we denote by $\min S$ the smallest integer $s \in S$, if one exists, and by $\inf S$ the largest integer $m \in \mathbb{Z}$ such that $m \leq s$, for all $s \in S$.

A *linear term* t over a set of variables in \mathbf{x} is a linear combination of the form $a_0 + \sum_{i=1}^n a_i x_i$, where $a_0, a_1, \dots, a_n \in \mathbb{Z}$. *Presburger arithmetic* is the first-order logic over propositions $t \leq 0$. Presburger arithmetic has quantifier elimination and is decidable [29]. For simplicity we consider only formulas in Presburger arithmetic in this paper.

For a first-order logical formula φ , let $FV(\varphi)$ denote the set of its free variables. By writing $\varphi(\mathbf{x})$ we imply that $FV(\varphi) \subseteq \mathbf{x}$. For a formula $\varphi(\mathbf{x})$, we denote by $\varphi[t_1/x_1, \dots, t_n/x_n]$ the formula obtained from φ by syntactically replacing each free occurrence of x_1, \dots, x_n with the terms t_1, \dots, t_n , respectively.

A *valuation* of \mathbf{x} is a function $\nu : \mathbf{x} \rightarrow \mathbb{Z}$. The set of all such valuations is denoted by $\mathbb{Z}^{\mathbf{x}}$. If $\nu \in \mathbb{Z}^{\mathbf{x}}$, we denote by $\nu \models \varphi$ the fact that the formula obtained from φ by replacing each occurrence of x_i with $\nu(x_i)$ is valid. Similarly, an arithmetic formula $R(\mathbf{x}, \mathbf{x}')$ defining a relation $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ is evaluated with respect to two valuations ν_1 and ν_2 , by replacing each occurrence of x_i with $\nu_1(x_i)$ and each occurrence of x'_i with $\nu_2(x'_i)$. The satisfaction relation is denoted $(\nu_1, \nu_2) \models R$. By $\models \varphi$ we denote the fact that φ is *valid* i.e., logically equivalent to true. We say that an arithmetic formula $\varphi(\mathbf{x})$ is *consistent* if there exists a valuation ν such that $\nu \models \varphi$. We use the symbols $\Rightarrow, \Leftrightarrow$ to denote logical implication and equivalence, respectively. The consistency of a formula φ is usually denoted by writing $\varphi \not\models \text{false}$. In the following, we will sometimes abuse the notation and use the same symbols for relations (sets) and their defining formulae.

The composition of two relations $R_1, R_2 \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ is defined as $R_1 \circ R_2 = \{(\nu, \nu') \in \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}} \mid \exists \nu'' \in \mathbb{Z}^{\mathbf{x}} . (\nu, \nu'') \in R_1 \wedge (\nu'', \nu') \in R_2\}$. For any relation $R \subseteq \mathbb{Z}^{\mathbf{x}}$, we consider R^0 to be the identity relation $\mathcal{I} = \{(\nu, \nu) \mid \nu \in \mathbb{Z}^{\mathbf{x}}\}$ and define $R^{i+1} = R^i \circ R$, for all $i \geq 0$. R^i is called the *i-th power* of R in the sequel. With these notations, $R^+ = \bigcup_{i=1}^{\infty} R^i$ denotes the *transitive closure* of R , and $R^* = R^+ \cup \mathcal{I}$ denotes the *reflexive and transitive closure* of R . The inverse of R is defined as $R^{-1} = \{(\nu', \nu) \mid (\nu, \nu') \in R\}$. The *inverse powers* of a relation R are defined inductively $R^{-i} = R^{-i+1} \circ R^{-1}$ for each $i \geq 1$. The post-image of a set $S \subseteq \mathbb{Z}^{\mathbf{x}}$ via a relation $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ is defined as $R(S) = \{\nu' \in \mathbb{Z}^{\mathbf{x}} \mid \exists \nu \in S . (\nu, \nu') \in R\}$. The pre-image of S via R is defined as $R^{-1}(S)$. A relation $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ is said to be *deterministic* if and only if $(\nu, \nu') \in R$ and $(\nu, \nu'') \in R$ implies $\nu' = \nu''$, for all $\nu, \nu', \nu'' \in \mathbb{Z}^{\mathbf{x}}$.

A function $F : 2^{\mathbb{Z}^{\mathbf{x}}} \rightarrow 2^{\mathbb{Z}^{\mathbf{x}}}$ is said to be *monotonic* if and only if $X \subseteq Y$ implies $F(X) \subseteq F(Y)$, for any two sets $X, Y \subseteq \mathbb{Z}^{\mathbf{x}}$, and \cap -*continuous* if and only if $F(\bigcap_{i=1}^{\infty} X_i) = \bigcap_{i=1}^{\infty} F(X_i)$, for any infinite sequence $\{X_i \subseteq \mathbb{Z}^{\mathbf{x}}\}_{i=1}^{\infty}$. The *greatest fixpoint* F is the largest set X such that $F(X) = X$, and is denoted $\text{gfp } F$. The function that maps each set $X \subseteq \mathbb{Z}^{\mathbf{x}}$ into its pre-image $R^{-1}(X)$ is denoted by pre_R in the following. It is easy to show that pre_R is monotonic, and that $\text{pre}_R^m = \text{pre}_{R^m}$, for all $m \geq 0$.

3. WEAKEST PRECONDITIONS FOR NON-TERMINATION

This section is concerned with the definition of weakest preconditions for non-termination, and the characterization of such preconditions as greatest fixpoints of the pre-image function. We also give certain conditions under which these fixpoints are computable as limits of descending Kleene sequences, and finally, define them using first-order integer arithmetic.

Let $\mathbf{x} = \{x_1, \dots, x_n\}$ be a set of variables interpreted over \mathbb{Z} . We start by defining the notions of **-consistent* and *well-founded* relations.

Definition 1. A relation $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ is said to be **-consistent* if and only if, for any $m > 0$, there exists a sequence of valuations $\{\nu_i \in \mathbb{Z}^{\mathbf{x}}\}_{i=0}^m$, such that $(\nu_i, \nu_{i+1}) \in R$, for all $i = 0, \dots, m-1$. R is said to be *well-founded* if and only if there is no infinite sequence of valuations $\{\nu_i \in \mathbb{Z}^{\mathbf{x}}\}_{i \geq 0}$, such that $(\nu_i, \nu_{i+1}) \in R$, for all $i \geq 0$.

Notice that if a relation is not **-consistent*, then it is also *well-founded*. However the dual is not true. For instance, the relation $R = \{(n, n-1) \mid n > 0\}$ is both **-consistent* and

well-founded. Also notice that a relation R is $*$ -consistent if and only if R^i is consistent for all $i \geq 0$.

Definition 2. A set $S \subseteq \mathbb{Z}^x$ is said to be a *non-termination precondition* for a relation $R \subseteq \mathbb{Z}^x \times \mathbb{Z}^x$ if and only if, for each $\nu \in S$ there exists an infinite sequence of valuations $\{\nu_i \in \mathbb{Z}^x\}_{i \geq 0}$ such that $\nu = \nu_0(\mathbf{x})$ and $(\nu_i, \nu_{i+1}) \in R$, for all $i \geq 0$.

If S_0, S_1, \dots are all non-termination preconditions for R , then the (possibly infinite) union $\bigcup_{i=0,1,\dots} S_i$ is a non-termination precondition for R as well. The set $\text{wnt}(R) = \bigcup \{S \in \mathbb{Z}^x \mid S \text{ is a non-termination precondition for } R\}$ is called the *weakest non-termination precondition* for R . A relation R is well-founded if and only if $\text{wnt}(R) = \emptyset$. A set S such that $S \cap \text{wnt}(R) = \emptyset$ is called a *termination precondition*.

Definition 3. A set $S \subseteq \mathbb{Z}^x$ is said to be *recurrent* for a relation $R \in \mathbb{Z}^x \times \mathbb{Z}^x$ if and only if $S \subseteq \text{pre}_R(S)$.

Notice that if S is a recurrent set for a relation R , then for each $\nu \in S$ there exists $\nu' \in S$ such that $(\nu, \nu') \in R$.

Proposition 1. Let $S_0, S_1, \dots \in \mathbb{Z}^x$ be a (possibly infinite) sequence of sets, all of which are recurrent for a relation $R \in \mathbb{Z}^x \times \mathbb{Z}^x$. Then their union $\bigcup_{i=0,1,\dots} S_i$ is recurrent for R as well.

Proof. For each i we have $S_i \subseteq \text{pre}_R(S_i) \subseteq \text{pre}_R(\bigcup_{j=0,1,\dots} S_j)$. The last inclusion is by the monotonicity of pre_R . Hence $\bigcup_{j=0,1,\dots} S_j \subseteq \text{pre}_R(\bigcup_{j=0,1,\dots} S_j)$. \square

The set $\text{wrs}(R) = \bigcup \{S \in \mathbb{Z}^x \mid S \text{ is a recurrent set for } R\}$ is called the *weakest recurrent set* for R . By Proposition 1, $\text{wrs}(R)$ is recurrent for R . The following lemma shows that in fact, this is exactly the set of valuations from which an infinite iteration is also possible.

Lemma 1. Given a relation $R \in \mathbb{Z}^x \times \mathbb{Z}^x$, the weakest recurrent set for R equals its weakest non-termination precondition.

Proof. “ $\text{wrs}(R) \subseteq \text{wnt}(R)$ ” Let $\nu_0 \in \text{wrs}(R)$ be a valuation. Then there exists $\nu_1 \in \text{wrs}(R)$ such that $(\nu_0, \nu_1) \in R$. Applying this argument infinitely many times, one can construct an infinite sequence $\nu_0, \nu_1, \nu_2, \dots$ such that $(\nu_i, \nu_{i+1}) \in R$, for all $i \geq 0$. Hence $\nu_0 \in \text{wnt}(R)$. “ $\text{wnt}(R) \subseteq \text{wrs}(R)$ ” Let $\nu_0 \in \text{wnt}(R)$ be a valuation and let $\nu_0, \nu_1, \nu_2, \dots$ be arbitrary infinite sequence such that $(\nu_i, \nu_{i+1}) \in R$, for all $i \geq 0$. Clearly, $\nu_1 \in \text{wnt}(R)$ too. Consequently, $\nu_0 \in \text{pre}_R(\text{wnt}(R))$ for each state $\nu_0 \in \text{wnt}(R)$ and hence, $\text{wnt}(R) \subseteq \text{pre}_R(\text{wnt}(R))$. Thus, $\text{wnt}(R)$ is a recurrent set and hence $\text{wnt}(R) \subseteq \text{wrs}(R)$. \square

Next we define the weakest recurrent set as the greatest fixpoint of the transition relation’s pre-image.

Lemma 2. Given a relation $R \in \mathbb{Z}^x \times \mathbb{Z}^x$, the weakest recurrent set for R is the greatest fixpoint of the function pre_R .

Proof. By the Knaster-Tarski Fixpoint Theorem, $\text{gfp } \text{pre}_R = \bigcup \{S \mid S \subseteq \text{pre}_R(S)\} = \text{wrs}(R)$. \square

The following lemma gives sufficient conditions under which $\text{wrs}(R)$ can be computed as the limit of the descending Kleene sequence: $\mathbb{Z}^x \supseteq \text{pre}_R(\mathbb{Z}^x) \supseteq \text{pre}_R^2(\mathbb{Z}^x) \supseteq \dots$

Lemma 3. Let $R \in \mathbb{Z}^x \times \mathbb{Z}^x$ be a relation such that either:

- (1) pre_R is \cap -continuous, or
- (2) $\text{pre}_R^{n_2}(\mathbb{Z}^x) = \text{pre}_R^{n_1}(\mathbb{Z}^x)$ for some $n_2 > n_1 \geq 0$, or
- (3) $\bigcap_{m \geq 0} \text{pre}_R^m(\mathbb{Z}^x) = \emptyset$.

Then, $\text{wrs}(R) = \bigcap_{m \geq 0} \text{pre}_R^m(\mathbb{Z}^x)$.

Proof. If (1) holds, one can apply the Kleene Fixpoint Theorem and conclude that $\text{wrs}(R) = \text{gfp}(\text{pre}_R) = \bigcap_{m \geq 0} \text{pre}_R^m(\mathbb{Z}^x)$. If (2) holds, by the monotonicity of pre_R , we have $\text{pre}_R^{n_1}(\mathbb{Z}^x) = \text{pre}_R^{n_1+1}(\mathbb{Z}^x) = \dots = \text{pre}_R^{n_2}(\mathbb{Z}^x)$. Hence, $\text{pre}_R^{n_1}(\mathbb{Z}^x) = \text{pre}_R^n(\mathbb{Z}^x)$, for all $n \geq n_1$, is a fixpoint of pre_R , and since $\text{gfp } \text{pre}_R = \text{wrs}(R) = \text{wnt}(R) \subseteq \bigcap_{m \geq 0} \text{pre}_R^m(\mathbb{Z}^x)$, it must be that $\text{gfp } \text{pre}_R = \bigcap_{m \geq 0} \text{pre}_R^m(\mathbb{Z}^x)$. If (3) holds, observe that $\text{wnt}(R) \subseteq \text{pre}_R^m(\mathbb{Z}^x)$ for each $m \geq 0$. Consequently,

$$\text{wrs}(R) = \text{wnt}(R) \subseteq \bigcap_{m \geq 0} \text{pre}_R^m(\mathbb{Z}^x) = \emptyset$$

Hence, $\text{wrs}(R) = \bigcap_{m \geq 0} \text{pre}_R^m(\mathbb{Z}^x) = \emptyset$ and the lemma holds. \square

In the next section, we show that Lemma 3 is applicable, for different reasons, to both octagonal and finite-monoid affine relations: octagonal relations are either well-founded (3), or their descending Kleene sequences stabilize (2), and linear affine relations are \cap -continuous (1). Thus one can compute the weakest non-termination precondition for these classes as the limit of a descending Kleene sequence.

Next, we show that, for relations satisfying one of the conditions of Lemma 3, one can also define the weakest non-termination precondition in first order arithmetic.

Definition 4. Let $R \in \mathbb{Z}^x \times \mathbb{Z}^x$ be a relation. The *closed form* of R is a formula $\widehat{R}(k, \mathbf{x}, \mathbf{x}')$ such that, for all $n \geq 0$ and all $\nu, \nu' \in \mathbb{Z}^x$:

$$\nu, \nu' \models \widehat{R}(n, \mathbf{x}, \mathbf{x}') \Leftrightarrow (\nu, \nu') \in R^n$$

Notice that the closed form of a relation is unique, up to logical equivalence. Using the closed form $\widehat{R}(\mathbf{x}, \mathbf{x}', k)$ of R , one can now define $\text{wrs}(R)$, if R meets one of the conditions of Lemma 3:

$$\text{wrs}(R) \equiv \forall k \geq 0 . \exists \mathbf{x}' . \widehat{R}(k, \mathbf{x}, \mathbf{x}') \quad (3.1)$$

One of the results of [8] is that the closed forms of octagonal and finite monoid affine relations are Presburger definable. Under the assumption (still to be proved) that these relations meet the requirements of Lemma 3, their weakest non-termination preconditions can be defined in Presburger arithmetic. Since Presburger arithmetic is decidable, the termination problems for octagonal and finite-monoid affine relations are decidable as well.

Example 1. Consider an octagonal relation $R(x, x') \equiv x \geq 0 \wedge x' = x - 1$. The closed form of R is $\widehat{R}(k, \mathbf{x}, \mathbf{x}') \equiv x \geq k - 1 \wedge x' = x - k$. Quantifier elimination yields $\text{wrs}(R) \equiv \forall k > 0 \exists x' . x \geq k - 1 \wedge x' = x - k \equiv \forall k \geq 0 . x \geq k - 1 \equiv \text{false}$. Hence the relation R is well-founded. \square

4. OCTAGONAL RELATIONS

Octagonal constraints (also known as Unit Two Variables Per Inequality or UTVPI, for short) appear in the context of abstract interpretation where they have been extensively studied as an abstract domain [26]. They are defined syntactically as a conjunctions of atomic propositions of the form $\pm x \pm y \leq c$, where x and y are variables and c is an integer constant. They are a generalization of the simpler notion of *difference bounds constraints*. Since most results on octagons rely on notions related to difference bounds constraints, we introduce the latter, for reasons of self-containment.

4.1. Difference Bounds Relations. Difference bounds constraints are known as *zones* in the context of timed automata verification [2] and abstract interpretation [26]. They are defined syntactically as conjunctions of atomic propositions of the form $x - y \leq c$, where x and y are variables and c is an integer constant. Difference bounds constraints can be represented as matrices and graphs. These matrices (graphs) have a canonical form, which is used for efficient inclusion checks, and can be computed by the classical Floyd-Warshall algorithm.

Difference bounds relations are relations defined by difference bounds constraints over primed and unprimed variables (e.g. $x - x' \leq 0$). Difference bounds relations have been studied by Comon and Jurski who showed, in [14], that their transitive closure is Presburger definable. Their proof was subsequently simplified in [11], using the notion of *zigzag* automata. Intuitively, a zigzag automaton corresponding to a difference bounds relation R is a finite weighted graph that encodes the constraints of R^m as minimal weight paths of length m . In [8], we showed that zigzag automata can be also used in proving *periodicity* of difference bounds relations, which allows to compute the closed form $\widehat{R}(k, \mathbf{x}, \mathbf{x}')$ efficiently. As we will show in this section, zigzag automata also play a crucial role in designing a PTIME algorithm computing the weakest termination sets, and in proving the existence of linear ranking functions for octagonal relations.

Definition 5. A formula $\phi(\mathbf{x})$ is a *difference bounds constraint* if it is equivalent to a finite conjunction of atomic propositions of the form $x_i - x_j \leq a_{ij}$, $1 \leq i, j \leq N, i \neq j$, where $a_{ij} \in \mathbb{Z}$.

For instance, $x - y = 5$ is a difference bounds constraint, as it is equivalent to $x - y \leq 5 \wedge y - x \leq -5$. In practice, difference bounds constraints are represented either as matrices or as graphs:

Definition 6. Let $\mathbf{x} = \{x_1, x_2, \dots, x_N\}$ be a set of variables ranging over \mathbb{Z} and $\phi(\mathbf{x})$ be a difference bounds constraint. Then a *difference bounds matrix* (DBM) representing ϕ is an $N \times N$ matrix M_ϕ such that:

$$(M_\phi)_{i,j} = \begin{cases} \alpha_{i,j} & \text{if } (x_i - x_j \leq \alpha_{i,j}) \in AP(\phi) \\ \infty & \text{otherwise} \end{cases}$$

Definition 7. Let $\mathbf{x} = \{x_1, x_2, \dots, x_N\}$ be a set of variables ranging over \mathbb{Z} and $\phi(\mathbf{x})$ be a difference bounds constraint. Then ϕ can be represented as a weighted graph $\mathcal{G}_\phi = (\mathbf{x}, \rightarrow)$, where each vertex corresponds to a variable, and there is an edge $x_i \xrightarrow{a_{ij}} x_j$ in \mathcal{G}_ϕ if and only if there exists a constraint $x_i - x_j \leq a_{ij}$ in ϕ . This graph is also called a *constraint graph*.

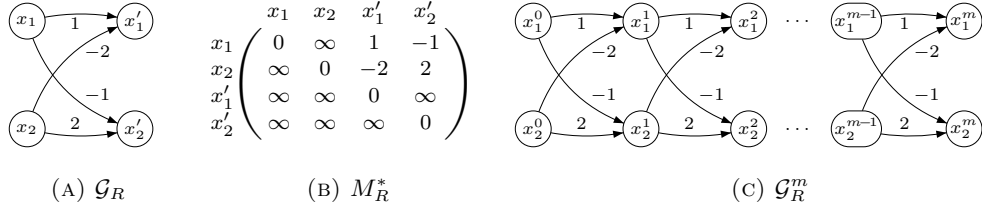


FIGURE 1. Graph and matrix representation of a relation. Graph unfolding.

Clearly, M_ϕ is the incidence matrix of \mathcal{G}_ϕ . If $M \in \mathbb{Z}_\infty^{N \times N}$ is a DBM, the corresponding difference bounds constraint is defined as $\Phi_M \Leftrightarrow \bigwedge_{M_{ij} < \infty} x_i - x_j \leq M_{ij}$. The restriction of a DBM M_ϕ to variables $\mathbf{z} \subseteq \mathbf{x}$, denoted as $(M_\phi)_{\downarrow \mathbf{z}}$, is a matrix obtained by erasing the rows and columns of M_ϕ . For two difference bounds matrices M_1, M_2 , we write $M_1 = M_2$ if and only if $(M_1)_{ij} = (M_2)_{ij}$ for all $1 \leq i, j \leq N$ and $M_1 \leq M_2$ if and only if $(M_1)_{ij} \leq (M_2)_{ij}$ for all $1 \leq i, j \leq N$.

A DBM M is said to be *consistent* if and only if its corresponding constraint ϕ_M is consistent. The next definition gives a canonical form for consistent DBMs.

Definition 8. A consistent DBM $M \in \mathbb{Z}_\infty^{N \times N}$ is said to be *closed* if and only if $M_{ii} = 0$ and $M_{ij} \leq M_{ik} + M_{kj}$, for all $1 \leq i, j, k \leq N$.

Given a consistent DBM $M \in \mathbb{Z}^N \times \mathbb{Z}^N$, we denote the closed DBM by M^* . It is well-known that, if M is consistent, then M^* is unique. The closed form is needed to check the equivalence and entailment of two difference bounds constraints.

Proposition 2 ([26]). Let ϕ_1 and ϕ_2 be consistent difference bounds constraints. Then,

- $\phi_1 \Leftrightarrow \phi_2$ if and only if $M_{\phi_1}^* = M_{\phi_2}^*$,
- $\phi_1 \Rightarrow \phi_2$ if and only if $M_{\phi_1}^* \leq M_{\phi_2}^*$.

Remark. The closed form of a consistent DBM $M \in \mathbb{Z}^N \times \mathbb{Z}^N$ can be computed in $\mathcal{O}(N^3)$ iterations, by the classical Floyd-Warshall algorithm [16]. Let μ denote the maximal absolute value among the entries of M . Since each iteration uses constantly many additions and comparisons, each of which involves absolute values at most $N \cdot \mu$, the time complexity of the closure computation is at most $\mathcal{O}(N^3 \cdot \log(N \cdot \mu))$. If M is inconsistent, then this can be detected, by a slightly improved version of Floyd-Warshall, with the same worst case time complexity. \square

A relation $R \in \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ is a *difference bounds relation* if it can be defined by a difference bounds constraint $R(\mathbf{x}, \mathbf{x}')$. It is well-known that the class of difference bounds relations is closed under relational composition [26].

Example 2. Let $R(x_1, x_2, x'_1, x'_2) \Leftrightarrow x_1 - x'_1 \leq 1 \wedge x_1 - x'_2 \leq -1 \wedge x_2 - x'_1 \leq -2 \wedge x_2 - x'_2 \leq 2$ be a difference bounds relation. Figure 1a shows the graph representation \mathcal{G}_R and Figure 1b the closed DBM representation of R . \square

Given a difference bounds relation $R(\mathbf{x}, \mathbf{x}')$, we define the m -times concatenation of \mathcal{G}_R with itself.

Definition 9. Let $R(\mathbf{x}, \mathbf{x}')$, $x = \{x_1, \dots, x_N\}$, be a difference bounds relation and \mathcal{G}_R be its constraint graph. The m -times unfolding of \mathcal{G}_R is defined as

$$\mathcal{G}_R^m = (\bigcup_{k=0}^N \mathbf{x}^{(k)}, \rightarrow),$$

where $\mathbf{x}^{(k)} = \{x_i^{(k)} \mid 0 \leq i \leq N\}$ and for all $0 \leq k < N$,

- $(x_i^{(k)} \xrightarrow{c} x_j^{(k)}) \in \rightarrow$ if and only if $(x_i - x_j \leq c) \in AP(\phi)$
- $(x_i^{(k)} \xrightarrow{c} x_j^{(k+1)}) \in \rightarrow$ if and only if $(x_i - x'_j \leq c) \in AP(\phi)$
- $(x_i^{(k+1)} \xrightarrow{c} x_j^{(k)}) \in \rightarrow$ if and only if $(x'_i - x_j \leq c) \in AP(\phi)$
- $(x_i^{(k+1)} \xrightarrow{c} x_j^{(k+1)}) \in \rightarrow$ if and only if $(x'_i - x'_j \leq c) \in AP(\phi)$

Each constraint in R^m corresponds to a path between extremal points in \mathcal{G}_R^m . Notice that, since difference bounds relations are closed under composition, then R^m is a difference bounds relation, for any $m > 0$. Then we have:

$$R^m \Leftrightarrow \bigwedge_{1 \leq i, j \leq N} x_i - x_j \leq \min\{x_i^0 \rightarrow x_j^0\} \wedge x'_i - x'_j \leq \min\{x_i^m \rightarrow x_j^m\} \wedge x_i - x'_j \leq \min\{x_i^0 \rightarrow x_j^m\} \wedge x'_i - x_j \leq \min\{x_i^m \rightarrow x_j^0\}$$

where $\min\{x_i^p \rightarrow x_j^q\}$ is the minimal weight between all paths among the extremal vertices x_i^p and x_j^q in \mathcal{G}_R^m , for $p, q \in \{0, m\}$.

Example 3. Figure 1c depicts the m -times unfolding of \mathcal{G}_R for the relation $R \Leftrightarrow x_1 - x'_1 \leq 1 \wedge x_1 - x'_2 \leq -1 \wedge x_2 - x'_1 \leq -2 \wedge x_2 - x'_2 \leq 2$. \square

The set of paths between any two extremal points in \mathcal{G}_R^m can be seen as words over the finite alphabet of subgraphs of \mathcal{G}_R^m that are accepted by a finite weighted automaton called *zigzag automaton* [11]. In the following section, we give the definition of these automata.

4.2. Zigzag Automata. This section defines zigzag automata, which can be seen as recognizers of powers of difference bounds relations. Intuitively, a zigzag automaton corresponding to a difference bounds relation R is a finite weighted automaton that encodes m -th power of R by minimal runs of length $m + 2$.

4.2.1. Alphabet and Words. Without losing generality, in the following we work with a simplified (yet equivalent) form of difference bounds relations: all constraints of the form $x - y \leq \alpha$ are replaced by $x - t' \leq \alpha \wedge t' - y \leq 0$, and all constraints of the form $x' - y' \leq \alpha$ are replaced by $x' - t \leq \alpha \wedge t - y' \leq 0$, by introducing fresh variables $t \notin \mathbf{x}$. In other words, we can assume that the constraint graph \mathcal{G}_R corresponding to R is *bipartite*, i.e. it does only contain edges from \mathbf{x} to \mathbf{x}' and vice versa.

A path π in \mathcal{G}_R^m between, say, x^0 and y^m , with $x, y \in \mathbf{x}$ is represented by a word $w = w_1 \dots w_m$ of length m , as follows: the w_i symbol represents *simultaneously* all edges of π that involve only nodes from $\mathbf{x}^{i-1} \cup \mathbf{x}^i$, $1 \leq i \leq m$. Since we assumed that \mathcal{G}_R^m is bipartite, it is easy to see that, for a path from x^0 to y^m , coded by a word w , the number of times

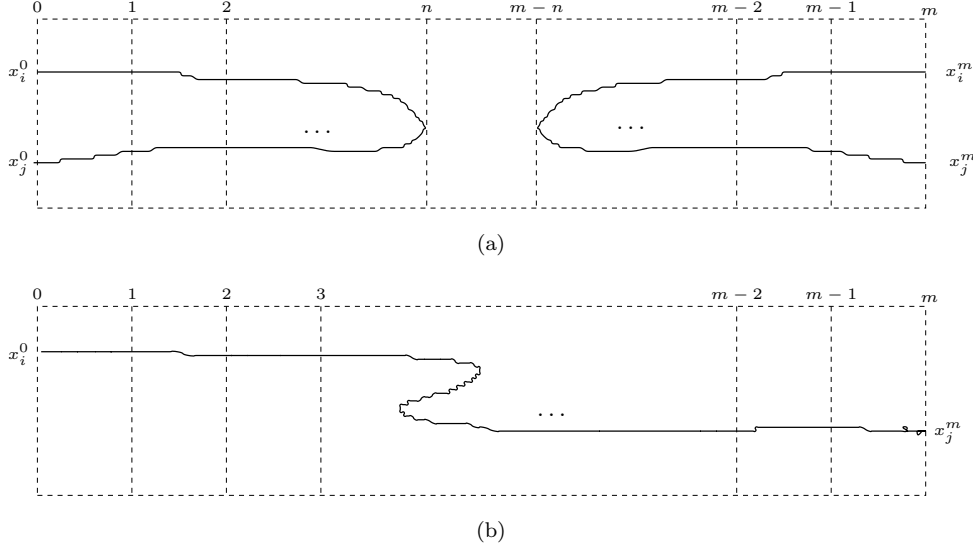


FIGURE 2. Runs of Even and Odd Automata

the w_i symbol is traversed by the path is odd, whereas for a path from x^0 to y^0 , or from x^m to y^m , this number is even. Hence the names of *even* and *odd automata*.

Given a difference bounds relation R , the *even alphabet* of R , denoted as Σ_R^e , is the set of all graphs satisfying the following conditions, for each $G \in \Sigma_R^e$:

- (1) the set of nodes of G is $\mathbf{x} \cup \mathbf{x}'$
- (2) for any $x, y \in \mathbf{x} \cup \mathbf{x}'$, there is an edge labeled with $\alpha \in \mathbb{Z}$ from x to y , only if the constraint $x - y \leq \alpha$ occurs in ϕ
- (3) the in-degree and out-degree of each node are at most one
- (4) the number of edges from \mathbf{x} to \mathbf{x}' equals the number of edges from \mathbf{x}' to \mathbf{x}

Notice that the number of edges in all symbols of Σ_R^e is even.

The *odd alphabet* of R , denoted by Σ_R^o , is defined in the same way, with the exception of the last condition, which becomes:

4. the difference between the number of edges from \mathbf{x} to \mathbf{x}' and the number of edges from \mathbf{x}' to \mathbf{x} is either 1 or -1

Notice that the number of edges in all symbols of Σ_R^o is odd.

Let $\Sigma_R = \Sigma_R^e \cup \Sigma_R^o \cup \{\epsilon\}$ be the alphabet of the zigzag automaton for R , where ϵ is a special symbol of weight 0. The weight of any symbol $G \in \Sigma_R^e \cup \Sigma_R^o$, denoted $\omega(G)$, is the sum of the weights that occur on its edges. For a word $w = w_1 w_2 \dots w_n \in \Sigma_R^*$, we define its weight as $\omega(w) = \sum_{i=1}^n \omega(w_i)$.

4.2.2. Construction of Zigzag Automata. We are now ready for the definition of automata recognizing words that represent encodings of paths from \mathcal{G}_R^m . The *even automaton* recognizes paths that start and end on the same side of \mathcal{G}_R^m i.e., either paths from x_i^0 to x_j^0 , or from x_i^m to x_j^m , for some $1 \leq i, j \leq N$, respectively. We call the automata recognizing paths from x_i^0 to x_j^0 *forward even automata*, and the ones recognizing paths from x_i^m to x_j^m *backward even automata* (Figure 2 (a)). The *odd automata* recognize paths from one side of \mathcal{G}_R^m to another. The automata recognizing paths from x_i^0 to x_j^m are called *forward*

odd automata, whereas the ones recognizing paths from x_i^m to x_j^0 are called *backward* odd automata (Figure 2 (b)).

The even and odd automata share the same alphabet and transition table, while the differences are in the sets of initial and final states. The common transition table is defined as $T_R = \langle Q, \Delta, w \rangle$, where Q is the set of control states defined as:

$$\begin{aligned} Q &= Q_g \cup \bigcup_{1 \leq i, j \leq N} (Q_{ij}^{ef} \cup Q_{ij}^{eb} \cup Q_{ij}^{of} \cup Q_{ij}^{ob}) \text{ where} \\ Q_g &= \{l, r, lr, rl, \perp\}^N \\ Q_{ij}^{ef} &= \{I_{ij}^{ef}, F_{ij}^{ef}\} & Q_{ij}^{eb} &= \{I_{ij}^{eb}, F_{ij}^{eb}\} \\ Q_{ij}^{of} &= \{I_i^{of}, F_j^{of}\} & Q_{ij}^{ob} &= \{I_i^{ob}, F_j^{ob}\} \end{aligned}$$

The $\{l, r, lr, rl, \perp\}$ components of states in Q_g capture the direction of incoming and outgoing edges (l for a path traversing from right to left, r for a path traversing from left to right, lr for a right incoming and right outgoing path, rl for a left incoming and left outgoing path, and \perp when there are no incoming nor outgoing edges from that node.). Given $1 \leq i, j \leq N$, the sets $Q_{ij}^{ef}, Q_{ij}^{eb}, Q_{ij}^{of}, Q_{ij}^{ob}$ contain the initial and the final state in even forward (ef), even backward (eb), odd forward (of), and odd backward (ob) zigzag automaton corresponding to i, j , respectively. The four automata recognize paths from $x_i^{(0)}$ to $x_j^{(0)}$ (ef), from $x_i^{(0)}$ to $x_j^{(0)}$ (eb), from $x_i^{(0)}$ to $x_j^{(m)}$ (of), and from $x_i^{(m)}$ to $x_j^{(0)}$ (ob) in \mathcal{G}_R^m , respectively.

The set of transitions Δ is defined as:

$$\Delta = \Delta_g \cup \Delta_l \bigcup_{1 \leq i, j \leq N} (\Delta_{ij}^{ef} \cup \Delta_{ij}^{eb} \cup \Delta_{ij}^{of} \cup \Delta_{ij}^{ob})$$

There is a transition

$$\langle q_1 \dots q_N \rangle \xrightarrow{G} \langle q'_1, \dots, q'_N \rangle$$

in Δ_g if and only if the following conditions hold, for all $1 \leq i \leq N$:

- $q_i = l$ iff G has one edge whose destination is x_i , and no other edge involving x_i .
- $q'_i = l$ iff G has one edge whose source is x'_i , and no other edge involving x'_i .
- $q_i = r$ iff G has one edge whose source is x_i , and no other edge involving x_i .
- $q'_i = r$ iff G has one edge whose destination is x'_i , and no other edge involving x'_i .
- $q_i = lr$ iff G has exactly two edges involving x_i , one having x_i as source, and another as destination.
- $q'_i = rl$ iff G has exactly two edges involving x'_i , one having x'_i as source, and another as destination.
- $q'_i \in \{lr, \perp\}$ iff G has no edge involving x'_i .
- $q_i \in \{rl, \perp\}$ iff G has no edge involving x_i .

Some even paths in \mathcal{G}_R^m may be of length strictly less than m . Since we want to recognize these path by runs of length $m+2$, we need several zero weight self-loop transitions:

$$\Delta_l = \{F^{ef} \xrightarrow{\epsilon} F^{ef}, I^{eb} \xrightarrow{\epsilon} I^{eb}\}$$

Finally, we define for each $q \leq i, j \leq N$ and each of the four zigzag automata (ef, eb, of, ob), the set of transitions that are incident with an initial or a final control state of the respective

automaton:

$$\begin{aligned}
\Delta_{ij}^{ef} &= \begin{cases} \{I_{ij}^{ef} \xrightarrow{\epsilon} q \mid q_i = r, q_j = l, q_h \in \{lr, \perp\}, 1 \leq h \leq N, h \notin \{i, j\}\} & \text{if } i \neq j \\ \{I_{ij}^{ef} \xrightarrow{\epsilon} q \mid q_i = q_j = lr, q_h \in \{lr, \perp\}, 1 \leq h \leq N, h \neq i\} & \text{if } i = j \end{cases} \\
&\cup \{q \xrightarrow{\epsilon} F^{ef} \mid q \in \{rl, \perp\}^N\} \\
\Delta_{ij}^{eb} &= \begin{cases} \{q \xrightarrow{\epsilon} F_{ij}^{eb} \mid q_i = l, q_j = r, q_h \in \{lr, \perp\}, 1 \leq h \leq N, h \notin \{i, j\}\} & \text{if } i \neq j \\ \{q \xrightarrow{\epsilon} F_{ij}^{eb} \mid q_i = q_j = lr, q_h \in \{lr, \perp\}, 1 \leq h \leq N, h \neq i\} & \text{if } i = j \end{cases} \\
&\cup \{I^{eb} \xrightarrow{\epsilon} q \mid q \in \{rl, \perp\}^N\} \\
\Delta_{ij}^{of} &= \{I_i^{of} \xrightarrow{\epsilon} q \mid q_i = r \text{ and } q_h \in \{lr, \perp\}, 1 \leq h \leq N, h \neq i\} \\
&\cup \{q \xrightarrow{\epsilon} F_j^{of} \mid q_j = r \text{ and } q_h \in \{rl, \perp\}, 1 \leq h \leq N, h \neq j\} \\
\Delta_{ij}^{ob} &= \{I_i^{ob} \xrightarrow{\epsilon} q \mid q_i = l \text{ and } q_h \in \{lr, \perp\}, 1 \leq h \leq N, h \neq i\} \\
&\cup \{q \xrightarrow{\epsilon} F_j^{ob} \mid q_j = l \text{ and } q_h \in \{rl, \perp\}, 1 \leq h \leq N, h \neq j\}
\end{aligned}$$

The weight function w maps each transition $q \xrightarrow{a} q' \in \Delta$, $q, q' \in Q$, $a \in \Sigma_R$ to $w(a)$.

Finally, for each $1 \leq i, j \leq N$, we define four zigzag automata

$$\begin{aligned}
A_{ij}^{ef} &= \langle Q, \Delta, w, I_{i,j}^{ef}, F^{ef} \rangle & A_{ij}^{of} &= \langle Q, \Delta, w, I_i^{of}, F_j^{of} \rangle \\
A_{ij}^{eb} &= \langle Q, \Delta, w, I^{eb}, F_{i,j}^{eb} \rangle & A_{ij}^{ob} &= \langle Q, \Delta, w, I_i^{ob}, F_j^{ob} \rangle
\end{aligned}$$

Notice that these automata share the same states and transitions, and the number of states is at most $5^N + 2N^2 + 4N + 2$, where N is the number of variables in \mathbf{x} .

In the following, we will sometimes shorthand paths in the zigzag automata of the form $q_1 \xrightarrow{a_1} q_1 \xrightarrow{a_2} \dots \xrightarrow{a_n} q_{n+1}$ as $q_1 \xrightarrow{a_1 \dots a_n} q_{n+1}$. Given words w_1, w_2, w_3 and paths $\pi_1 = q_1 \xrightarrow{w_1} q_2$, $\pi_2 = q_2 \xrightarrow{w_2} q_3$, $\pi_3 = q_3 \xrightarrow{w_3} q_4$, we write $\pi = \pi_1 \cdot \pi_2 \cdot \pi_3$ to denote the concatenated path $q_1 \xrightarrow{w_1} q_2 \xrightarrow{w_2} q_3 \xrightarrow{w_3} q_4$. We sometimes abuse the notation slightly and write π as e.g. $q_1 \xrightarrow{w_1} q_2 \xrightarrow{\pi_2} q_3 \xrightarrow{w_3} q_4$.

4.2.3. Language of Zigzag Automata. Recall that \mathcal{G}_R^m denotes the constraint graph corresponding to R^m , obtained by concatenating the constraint graph of R to itself $m > 0$ times. We say that a path in \mathcal{G}_R^m *stretches between k and l* , for some $k \leq l$, if the path contains at least one node from \mathbf{x}^i , for each $k \leq i \leq l$ and contains no node from \mathbf{x}^i , for each i such that $i < k$ or $i > l$. Intuitively, all paths from x_i^0 to x_j^0 in \mathcal{G}_R^m are recognized by the automaton A_{ij}^{ef} , paths from x_i^m to x_j^m by A_{ij}^{eb} (Figure 2 (a)), paths from x_i^0 to x_j^m by A_{ij}^{of} , and paths from x_i^m to x_j^0 by A_{ij}^{ob} (Figure 2 (b)). The following lemma makes the relationship between paths in \mathcal{G}_R^m and runs in zigzag automata of length $m + 2$ precise.

Lemma 4 ([11]). Suppose that \mathcal{G}_R^m does not have cycles of negative weight, for some $m > 0$. Then, for any $1 \leq i, j \leq N$, $i \neq j$, the following hold:

- (1) A_{ij}^{ef} has an accepting run of length $m + 2$ if and only if there exists a path in \mathcal{G}_R^m , from x_i^0 to x_j^0 , that stretches between 0 and n , for some $0 \leq n \leq m$. Moreover, the minimal weight among all paths from x_i^0 to x_j^0 in \mathcal{G}_R^m , stretching from 0 to n , for some $0 \leq n \leq m$, equals the minimal weight among all accepting runs of A_{ij}^{ef} of length $m + 2$.
- (2) A_{ij}^{eb} has an accepting run of length $m + 2$ if and only if there exists a path in \mathcal{G}_R^m , from x_i^m to x_j^m , that stretches between n and m , for some $0 \leq n \leq m$. Moreover, the minimal weight among all paths from x_i^m to x_j^m in \mathcal{G}_R^m , stretching from n to m , for some $0 \leq n \leq m$, equals the minimal weight among all accepting runs of A_{ij}^{eb} , of length $m + 2$.
- (3) A_{ij}^{of} has an accepting run of length $m + 2$ if and only if there exists a path in \mathcal{G}_R^m , from x_i^0 to x_j^m . Moreover, the minimal weight among all paths from x_i^0 to x_j^m in \mathcal{G}_R^m equals the minimal weight among all accepting runs of length $m + 2$.
- (4) A_{ij}^{ob} has an accepting run of length $m + 2$ if and only if there exists a path in \mathcal{G}_R^m , from x_i^m to x_j^0 . Moreover, the minimal weight among all paths from x_i^m to x_j^0 in \mathcal{G}_R^m equals the minimal weight among all accepting runs of length $m + 2$.

Proof. See [11], Lemmas 4.3, 4.4, 4.6 and 4.7. \square

Example 4. Let us show the construction of the zigzag automaton for the relation $R \Leftrightarrow x_1 - x'_1 \leq 1 \wedge x_1 - x'_2 \leq -1 \wedge x_2 - x'_1 \leq -2 \wedge x_2 - x'_2 \leq 2$. Figures 2(a) and (b) depict \mathcal{G}_R and M_R^* . Notice that there are only forward odd paths, i.e. paths from \mathbf{x}_0 to \mathbf{x}_m in \mathcal{G}_R^m for any $m \geq 1$. The transition table $T_R = \langle Q, \Delta, w \rangle$ of the zigzag automaton is depicted in Figure 3 (isolated states, such as (r, l) , have been removed). For instance, the automaton $A_{xy}^{ef} = \langle T_R, I_x^{of}, F_x^{of} \rangle$ recognizes a run of length $m + 2$ with weight w if and only if there is a path from x_0 to x^m in \mathcal{G}_R^m of length m and with weight w . There are four such paths in \mathcal{G}_R^3 and the Figure 4 shows the corresponding runs of the zigzag automaton. The second and the third runs have minimal weight. \square

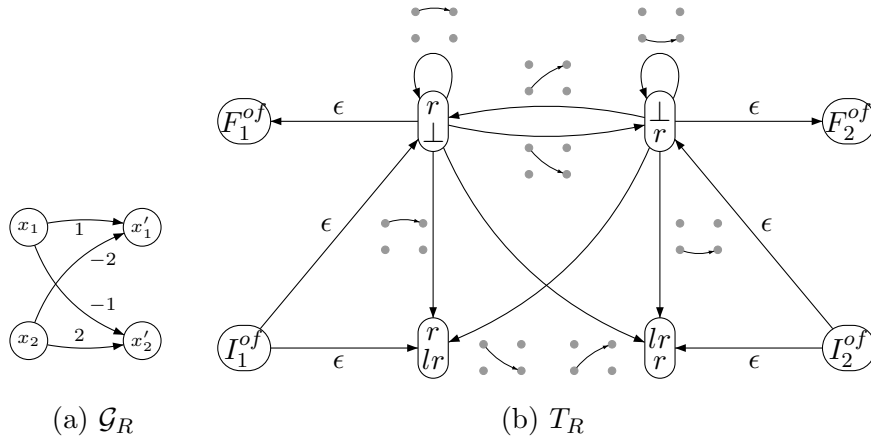


FIGURE 3. Zigzag automaton

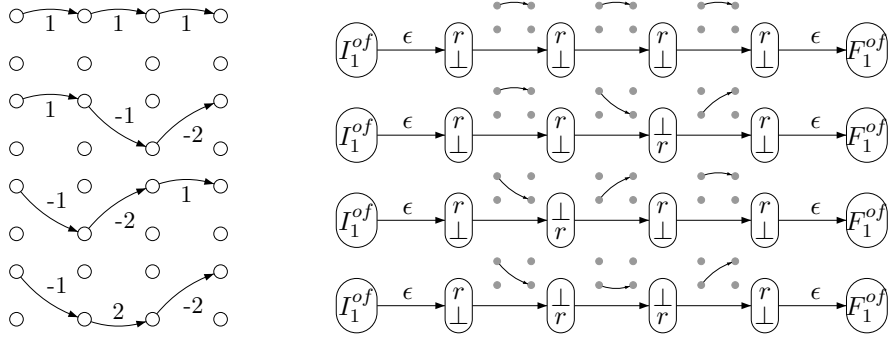


FIGURE 4. Runs

4.3. Octagonal Constraints. Octagonal constraints are a generalization of difference bounds constraints to conjunctions of atomic propositions of the form $\pm x \pm y \leq c$, $c \leq \mathbb{Z}$. An octagonal constraint $\phi(x_1, \dots, x_N)$ is usually represented by a difference bounds constraints $\phi(y_1, \dots, y_{2N})$ where y_{2i-1} stands for $+x_i$ and y_{2i} stands for $-x_i$, with the implicit requirement that $y_{2i-1} = -y_{2i}$, for each $1 \leq i \leq N$. With this convention, [4] provides an algorithm for computing the canonical form of an octagon by first computing the canonical form of the corresponding difference bounds constraint and subsequently *tightening* the difference bounds constraints $y_i - y_j \leq c$.

The problem of computing the closed forms of octagonal relations was studied first in [7] where it was shown that the closed forms of octagonal relations are Presburger definable. The core result of [7] is that the canonical form of the m -th power of an octagonal relation R can be computed directly from the m -th power of a difference bounds relation that represents R . For self-containment reasons, we present these results in Section 4.4.

Let $\mathbf{x} = \{x_1, x_2, \dots, x_N\}$ be a set of variables ranging over \mathbb{Z} . The class of integer octagonal constraints is defined as follows:

Definition 10. A formula $\phi(\mathbf{x})$ is an *octagonal constraint* if it is equivalent to a finite conjunction of terms of the form $x_i - x_j \leq a_{ij}$, $x_i + x_j \leq b_{ij}$ or $-x_i - x_j \leq c_{ij}$ where $a_{ij}, b_{ij}, c_{ij} \in \mathbb{Z}$, for all $1 \leq i, j \leq N$.

We represent octagons as difference bounds constraints over the dual set of variables $\mathbf{y} = \{y_1, y_2, \dots, y_{2N}\}$, with the convention that y_{2i-1} stands for x_i and y_{2i} for $-x_i$, respectively. For example, the octagonal constraint $x_1 + x_2 = 3$ is represented as $y_1 - y_4 \leq 3 \wedge y_2 - y_3 \leq -3$. In order to handle the \mathbf{y} variables in the following, we define $\bar{i} = i - 1$, if i is even, and $\bar{i} = i + 1$ if i is odd. Obviously, we have $\bar{\bar{i}} = i$, for all $i \in \mathbb{Z}$, $i \geq 0$. We denote by $\bar{\phi}(\mathbf{y})$ the difference bounds constraint over \mathbf{y} that represents $\phi(\mathbf{x})$ and which is defined as follows:

Definition 11. Given an octagonal constraint $\phi(\mathbf{x})$, $\mathbf{x} = \{x_1, \dots, x_N\}$, its difference bounds representation $\bar{\phi}(\mathbf{y})$, $\mathbf{y} = \{y_1, \dots, y_{2N}\}$ is a conjunction of the following difference bounds constraints where $1 \leq i \neq j \leq N$, $c \in \mathbb{Z}$.

$$\begin{aligned}
 (x_i - x_j \leq c) \in AP(\phi) &\Leftrightarrow (y_{2i-1} - y_{2j-1} \leq c), (y_{2j} - y_{2i} \leq c) \in AP(\bar{\phi}) \\
 (-x_i + x_j \leq c) \in AP(\phi) &\Leftrightarrow (y_{2j-1} - y_{2i-1} \leq c), (y_{2i} - y_{2j} \leq c) \in AP(\bar{\phi}) \\
 (-x_i - x_j \leq c) \in AP(\phi) &\Leftrightarrow (y_{2i} - y_{2j-1} \leq c), (y_{2j} - y_{2i-1} \leq c) \in AP(\bar{\phi}) \\
 (x_i + x_j \leq c) \in AP(\phi) &\Leftrightarrow (y_{2i-1} - y_{2j} \leq c), (y_{2j-1} - y_{2i} \leq c) \in AP(\bar{\phi}) \\
 (2x_i \leq c) \in AP(\phi) &\Leftrightarrow (y_{2i-1} - y_{2i} \leq c) \in AP(\bar{\phi}) \\
 (-2x_i \leq c) \in AP(\phi) &\Leftrightarrow (y_{2i} - y_{2i-1} \leq c) \in AP(\bar{\phi})
 \end{aligned}$$

Given an octagonal constraint $\phi(\mathbf{x})$ and its difference bounds representation $\bar{\phi}(\mathbf{y})$, we define $\hat{\hat{\phi}}(\mathbf{x})$ as

$$\hat{\hat{\phi}}(\mathbf{x}) \Leftrightarrow (\exists y_2, y_4, \dots, y_{2N} \cdot \bar{\phi} \wedge \bigwedge_{i=1}^N y_{2i-1} = -y_{2i}) [x_i/y_{2i-1}]_{i=1}^N \quad (4.1)$$

Clearly, it follows that

$$\phi(\mathbf{x}) \Leftrightarrow \hat{\hat{\phi}}(\mathbf{x}) \Leftrightarrow (\exists y_2, y_4, \dots, y_{2N} \cdot \bar{\phi} \wedge \bigwedge_{i=1}^N y_{2i-1} = -y_{2i}) [x_i/y_{2i-1}]_{i=1}^N \quad (4.2)$$

An octagonal constraint ϕ is equivalently represented by the DBM $M_{\bar{\phi}} \in \mathbb{Z}_{\infty}^{2N \times 2N}$, corresponding to $\bar{\phi}$. We sometimes write M_{ϕ} instead of $M_{\bar{\phi}}$. We say that a DBM $M \in \mathbb{Z}_{\infty}^{2N \times 2N}$ is *coherent* iff $M_{ij} = M_{\bar{j}}$ for all $1 \leq i, j \leq 2N$. This property is needed since e.g. an atomic proposition $x_i - x_j \leq a_{ij}$, $1 \leq i, j \leq N$, can be represented as both $y_{2i-1} - y_{2j-1} \leq a_{ij}$ and $y_{2j} - y_{2i} \leq a_{ij}$. Dually, a coherent DBM $M \in \mathbb{Z}_{\infty}^{2N \times 2N}$ corresponds to the octagonal constraint:

$$\Omega_M \Leftrightarrow \bigwedge_{1 \leq i, j \leq N} (x_i - x_j \leq M_{2i-1, 2j-1} \wedge x_i + x_j \leq M_{2i-1, 2j} \wedge -x_i - x_j \leq M_{2i, 2j-1}) \quad (4.3)$$

A coherent DBM M is said to be *octagonal-consistent* if and only if Ω_M is consistent.

Definition 12. An octagonal-consistent coherent DBM $M \in \mathbb{Z}_{\infty}^{2N \times 2N}$ is said to be *tightly closed* if and only if the following hold, for all $1 \leq i, j, k \leq 2N$:

1. $M_{ii} = 0$
2. $M_{i\bar{i}}$ is even
3. $M_{ij} \leq M_{ik} + M_{kj}$
4. $M_{ij} \leq \lfloor \frac{M_{i\bar{i}}}{2} \rfloor + \lfloor \frac{M_{\bar{j}j}}{2} \rfloor$

Given an octagonal-consistent coherent DBM $M \in \mathbb{Z}^{2N} \times \mathbb{Z}^{2N}$, we denote the (unique) tightly closed DBM by M^t . The following theorem from [4] provides an effective way of testing octagonal-consistency and computing the tight closure of a coherent DBM. Moreover, it shows that the tight closure of a given DBM is unique and can also be computed with the same worst-case time complexity as the DBM closure.

Theorem 1. ([4]) Let $M \in \mathbb{Z}_{\infty}^{2N \times 2N}$ be a coherent DBM. Then M is octagonal-consistent if and only if M is consistent and $\lfloor \frac{M_{i\bar{i}}^*}{2} \rfloor + \lfloor \frac{M_{\bar{j}j}^*}{2} \rfloor \geq 0$, for all $1 \leq i \leq 2N$. Moreover, if M is octagonal-consistent, the tight closure of M is the DBM $M^t \in \mathbb{Z}_{\infty}^{2N \times 2N}$ defined as:

$$M_{ij}^t = \min \left\{ M_{ij}^*, \left\lfloor \frac{M_{i\bar{i}}^*}{2} \right\rfloor + \left\lfloor \frac{M_{\bar{j}j}^*}{2} \right\rfloor \right\}$$

for all $1 \leq i, j \leq 2N$ where $M^* \in \mathbb{Z}_{\infty}^{2N \times 2N}$ is the closure of M .

The tight closure of DBMs is needed for checking equivalence and entailment between octagonal constraints. Two octagonal constraints are equivalent if and only if their tight DBMs are equal. Moreover, octagonal constraints are closed under existential quantification.

Proposition 3. (Theorem 2 in [7]) Let $\phi(\mathbf{x})$, $\mathbf{x} = \{x_1, \dots, x_N\}$, be an octagonal-consistent octagonal constraint. Further, let $1 \leq k \leq 2N$ and M' be the restriction of M_{ϕ}^t to $\mathbf{y} \setminus \{y_{2k-1}, y_{2k}\}$. Then, M' is tightly closed, and $\Omega(M') \Leftrightarrow \exists x_k. \phi(\mathbf{x})$.

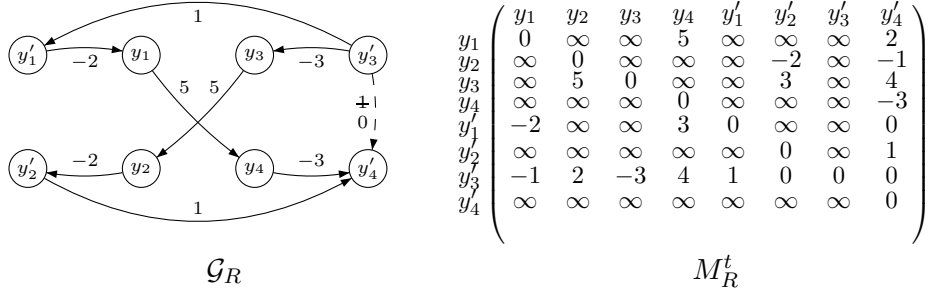


FIGURE 5. Graph and matrix representation of a relation.

4.4. The Powers of Octagonal Relations. A relation $R \subseteq \mathbb{Z}^x \times \mathbb{Z}^x$ over a set of variables is an *octagonal relation* if it can be defined by an octagonal constraint $R(\mathbf{x}, \mathbf{x}')$.

Example 5. Consider the octagonal relation $R(x_1, x_2, x'_1, x'_2) \Leftrightarrow x_1 + x_2 \leq 5 \wedge x'_1 - x_1 \leq -2 \wedge x'_2 - x_2 \leq -3 \wedge x'_2 - x'_1 \leq 1$. Its difference bounds representation is $\bar{R}(\mathbf{y}, \mathbf{y}') \Leftrightarrow y_1 - y_4 \leq 5 \wedge y_3 - y_2 \leq 5 \wedge y'_1 - y_1 \leq -2 \wedge y_2 - y'_2 \leq -2 \wedge y'_3 - y_3 \leq -3 \wedge y_4 - y'_4 \leq -3 \wedge y'_3 - y'_1 \leq 1 \wedge y'_2 - y'_4 \leq 1$, where $\mathbf{y} = \{y_1, \dots, y_4\}$. Figure 5a shows the graph representation \mathcal{G}_R . Note that the implicit constraint $y'_3 - y'_4 \leq 1$ (represented by a dashed edge in Figure 5a) is not tight. The tightening step replaces the bound 1 (crossed in Figure 5a) with 0. Figure 5b shows the tightly closed DBM representation of R , denoted M_R^t . \square

A consequence of Proposition 3 is that octagonal relations are closed under relational composition [7]. We need here the main result of [7] which establishes the following relation between $M_{R^m}^t$ (the tightly closed octagonal DBM corresponding to the m -th iteration of R) and $M_{\bar{R}}^*$ (the closed DBM corresponding to the m -th iteration of the difference bounds relation \bar{R}), for all $m \geq 0$:

Theorem 2. ([7]) Let $R(\mathbf{x}, \mathbf{x}')$, $\mathbf{x} = \{x_1, \dots, x_N\}$, be a $*$ -consistent octagonal relation. Then, $M_{R^m}^t = M_{\bar{R}}^*$ for all $m \geq 0$. Consequently,

$$(M_{R^m}^t)_{ij} = \min \left\{ (M_{\bar{R}}^*)_{ij}, \left\lfloor \frac{(M_{\bar{R}}^*)_{i\bar{i}}}{2} \right\rfloor + \left\lfloor \frac{(M_{\bar{R}}^*)_{\bar{j}j}}{2} \right\rfloor \right\}$$

for all $1 \leq i, j \leq 4N$.

The statement of Theorem 2 is in fact a generalization of the tight closure definition from Theorem 1, from $m = 1$ to any $m \geq 0$.

Corollary 1. Let $R(\mathbf{x}, \mathbf{x}')$, $\mathbf{x} = \{x_1, \dots, x_N\}$ be a $*$ -consistent octagonal relation and $\bar{R}(\mathbf{y}, \mathbf{y}')$ its difference bounds representation. Then, for all $m \geq 0$ and $1 \leq i \leq N$:

- $R^m \Leftrightarrow \widehat{\bar{R}}^m$
- $\exists x_i . R^m \Leftrightarrow \exists y_{2i-1}, y_{2i} . \bar{R}^m$
- $\exists x'_i . R^m \Leftrightarrow \exists y'_{2i-1}, y'_{2i} . \bar{R}^m$

Proof. The fact that $R^m \Leftrightarrow \widehat{\bar{R}}^m$ for all $m \geq 0$ follows immediately from Theorem 2, since the computation of $M_{\bar{R}}^*$ and of $M_{R^m}^t$ infers constraints that are logical consequences of \bar{R}^m . For the second statement, note that $(M_{R^m}^t)_{\downarrow \mathbf{y} \cup \mathbf{y}' \setminus \{y_{2i-1}, y_{2i}\}}$ is computed as a function

of $(M_{\widehat{R}}^*)_{\downarrow \mathbf{y} \cup \mathbf{y}' \setminus \{y_{2i-1}, y_{2i}\}}$ by Theorem 2 and variables y_{2i-1}, y_{2i} can be thus eliminated before the tightening step. The argument for the third statement is analogical. \square

4.5. Computing Weakest Non-termination Sets in Polynomial Time. We first introduce a result from [8] that defines the “shape” of the closed form $\widehat{R}(k, \mathbf{x}, \mathbf{x}')$ for an octagonal relation R . Intuitively, for each $i \geq 0$, R^i is an octagon, whose bounds evolve in a periodic way. The following definition gives the precise meaning of periodicity for relations that have a matrix representation.

Definition 13. An infinite sequence of matrices $\{M_k\}_{k=1}^\infty \in \mathbb{Z}_\infty^{m \times m}$ is said to be *periodic* if and only if:

$$\exists b > 0 \exists c > 0 \exists \Lambda_0, \Lambda_1, \dots, \Lambda_{c-1} \in \mathbb{Z}_\infty^{m \times m} \cdot M_{b+(k+1)c+i} = \Lambda_i + M_{b+kc+i}$$

for all $k \geq 0$ and $i = 0, 1, \dots, c-1$. The smallest b, c for which the above holds are called *prefix* and *period* of the $\{M_k\}_{k=1}^\infty$ sequence, respectively.

A result reported in [8] is that the sequence $\{M_{R^i}^t\}_{i \geq 0}$ of tightly closed matrices representing the sequence $\{R^i\}_{i \geq 0}$ of powers of a $*$ -consistent octagonal relation R is periodic, in the sense of the above definition. The constants b and c from Definition 13 will also be called the *prefix and period of the octagonal relation R* , throughout this section.

In the subsequent developments, we rely on the following lemma (see [10] for the proof) that states a property of the rate Λ_0 of an octagonal relation.

Lemma 5. Let R be a $*$ -consistent octagonal relation with prefix b , period c , and rates $\Lambda_0, \dots, \Lambda_{c-1}$. Then, the DBM $n \cdot \Lambda_0 + M_{R^b}^t$ is tightly closed for all $n \geq 0$.

For a set \mathbf{v} of variables, let $U(\mathbf{v}) = \{\pm v_1 \pm v_2 \mid v_1, v_2 \in \mathbf{v}\}$ denote the set of octagonal terms over \mathbf{v} . As a first remark, by the periodicity of the sequence $\{M_{R^i}^t\}_{i \geq 0}$, the closed form of the subsequence $\{R^{b+c\ell}\}_{\ell \geq 0}$ (of $\{R^i\}_{i \geq 0}$) can be defined as:

$$\widehat{R}_{b,c}(\ell, \mathbf{x}, \mathbf{x}') \equiv \bigwedge_{u \in U(\mathbf{x} \cup \mathbf{x}')} u \leq a_u \ell + d_u \quad (4.4)$$

where $a_u = (\Lambda_0)_{ij}$, $d_u = (M_{R^b}^t)_{ij}$ for all octagonal terms $u = y_i - y_j$. This is indeed the case, since the matrix sequence $\{M_{R^{b+c\ell}}^t\}_{\ell \geq 0}$ is periodic i.e., $M_{R^{b+c\ell}}^t = M_{R^b}^t + \ell \Lambda_0$, for all $\ell \geq 0$.

Lemma 6. Let $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ be a $*$ -consistent octagonal relation with prefix b , period c and let $\widehat{R}_{b,c}(\ell, \mathbf{x}, \mathbf{x}')$ be the closed form of $\{R^{b+c\ell}\}_{\ell \geq 0}$ as defined in (4.4). Then, $\text{wrs}(R) = \bigcap_{k \geq 0} R^{-k}(\mathbb{Z}^{\mathbf{x}})$. Moreover, $\text{wrs}(R) = \emptyset$ if there exists $u \in U(\mathbf{x})$ such that $a_u < 0$. Otherwise, $\text{wrs}(R) = R^{-b}(\mathbb{Z}^{\mathbf{x}})$.

Proof. Notice that the function pre_R is monotonic and thus, $R^{-k_1}(\mathbb{Z}^{\mathbf{x}}) \supseteq R^{-k_2}(\mathbb{Z}^{\mathbf{x}})$, for $k_1 \leq k_2$. Consequently, we have that $\bigcap_{k > 0} R^{-k}(\mathbb{Z}^{\mathbf{x}}) = \bigcap_{\ell \geq 0} R^{-(b+c\ell)}(\mathbb{Z}^{\mathbf{x}})$. The latter set can now be defined using the closed form of the subsequence (4.4) i.e.,

$$\bigcap_{k > 0} R^{-k}(\mathbb{Z}^{\mathbf{x}}) \equiv \forall \ell \geq 0 \exists \mathbf{x}' \cdot \widehat{R}_{b,c}(\ell, \mathbf{x}, \mathbf{x}')$$

By Lemma 5, the DBM $n \cdot \Lambda_0 + M_{R^b}^t$ is tightly closed for all $n \geq 0$. Thus, the DBM encoding of $\widehat{R}_{b,c}(\ell, \mathbf{x}, \mathbf{x}')[n/\ell]$ is tightly closed for all $n \geq 0$. By Proposition 3, it follows that

the existential quantifier $\exists \mathbf{x}'$ can be eliminated by simply deleting all atomic propositions involving primed variables from (4.4). Thus, we obtain:

$$\begin{aligned} \bigcap_{k>0} R^{-k}(\mathbb{Z}^{\mathbf{x}}) &\equiv \forall \ell \geq 0 \bigwedge_{u \in U(\mathbf{x})} u \leq a_u \ell + d_u \\ &\equiv \bigwedge_{u \in U(\mathbf{x})} u \leq \inf \{a_u \ell + d_u \mid \ell \geq 0\} \end{aligned}$$

where, for a set $S \subseteq \mathbb{Z}$, $\inf S$ denotes the minimal element of S , if one exists, or $-\infty$, otherwise. We have

$$\inf \{a_u \ell + d_u \mid \ell \geq 0\} = \begin{cases} -\infty & \text{if } a_u < 0, \\ d_u & \text{otherwise.} \end{cases}$$

Hence $\bigcap_{k>0} R^{-k}(\mathbb{Z}^{\mathbf{x}})$ is the empty set, if $a_u < 0$ for some $u \in U(\mathbf{x})$. In this case, condition 3 of Lemma 3 holds. Otherwise, we obtain $\bigcap_{k>0} R^{-k}(\mathbb{Z}^{\mathbf{x}}) \equiv \bigwedge_{u \in U(\mathbf{x})} u \leq d_u$. However, this is exactly the set $R^{-b}(\mathbb{Z}^{\mathbf{x}})$, by (4.4). In this case, condition 2 of Lemma 3 holds. Thus, we can apply Lemma 3 in both cases and conclude that $\text{wrs}(R) = \bigcap_{k>0} R^{-k}(\mathbb{Z}^{\mathbf{x}})$. To summarize, $\text{wrs}(R) = \emptyset$ if $a_u < 0$ for some $u \in U(\mathbf{x})$. Otherwise, $\text{wrs}(R) = R^{-b}(\mathbb{Z}^{\mathbf{x}})$. \square

An immediate consequence is that the termination problem is decidable and that the weakest termination set is an effectively computable Presburger formula.

Theorem 3. The termination problem is decidable for octagonal relations. Moreover, the weakest non-termination set of an octagonal relation is an effectively computable octagonal constraint.

Proof. By Lemma 6, the weakest non-termination set of an octagonal relation is either empty or $R^{-b}(\mathbb{Z}^N)$. Moreover, Lemma 6 gives means to compute this set. Thus, the termination problem can be decided by checking whether $\text{wrs}(R) = \emptyset$. \square

The following proposition relates values of entries in $(M_{\overline{R}}^*)_{\downarrow \mathbf{y}}$ to weights of runs of length $k+2$ in the even forward zigzag automata.

Proposition 4. Let $R(\mathbf{x}', \mathbf{x})$, $\mathbf{x} = \{x_1, \dots, x_N\}$, be a $*$ -consistent octagonal relation, $\overline{R}(\mathbf{y}, \mathbf{y}')$, $\mathbf{y} = \{y_1, \dots, y_{2N}\}$, be a difference bounds representation of $R(\mathbf{x}', \mathbf{x})$, and let $\mathcal{A}_{\overline{R}}^{ef}$ be the even forward zigzag automaton corresponding to $\overline{R}(\mathbf{y}, \mathbf{y}')$. Then, the following assertions are equivalent for all $1 \leq i, j \leq 2N$ and all $m \geq 0$,

- (1) there exists an acyclic path ρ from $y_i^{(0)}$ to $y_j^{(0)}$ in $\mathcal{G}_{\overline{R}}^m$
- (2) there exists a run π in $\mathcal{A}_{\overline{R}}^{ef}$ of length $m+2$ such that $w(\pi) = w(\rho)$ and π is of the form $\pi = I_{i,j}^{ef} \xrightarrow{\epsilon} q \xrightarrow{\sigma} q' \xrightarrow{\epsilon} F^{ef} \xrightarrow{\epsilon^n} F^{ef}$ where $q, q' \in \{l, r, lr, rl, \perp\}^{2N}$ are control states, $n \geq 0$, and $w(\pi) = w(\sigma)$.

and moreover, $(M_{\overline{R}}^*)_{i,j} \leq w(\pi)$ for each path π of the above form. Moreover, there exists a path π of the above form such that $w(\pi) = (M_{\overline{R}}^*)_{i,j}$.

Proof. Follows from construction of $\mathcal{A}_{\overline{R}}^{ef}$ and the fact that $(M_{\overline{R}}^*)_{i,j}$ is the weight of the minimal weight path from $y_i^{(0)}$ to $y_j^{(0)}$ in $\mathcal{G}_{\overline{R}}^m$, by Lemma 4. \square

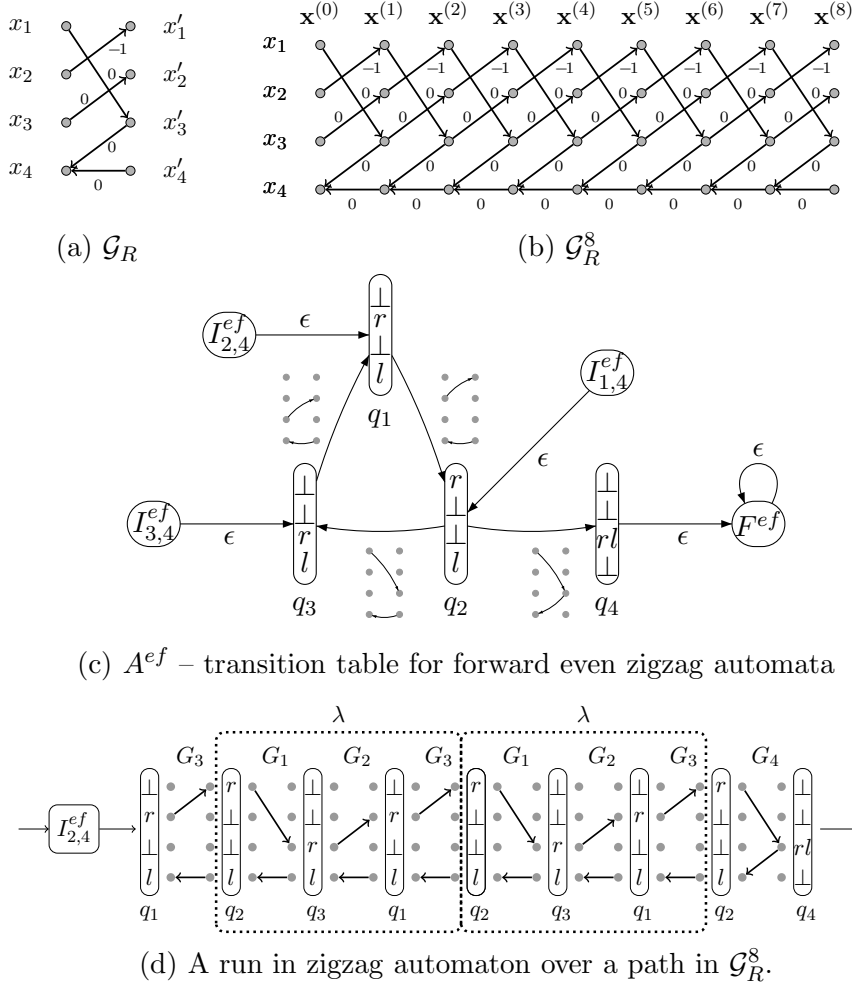


FIGURE 6. (a) \mathcal{G}_R – graph representation of $R(\mathbf{x}, \mathbf{x}')$. (b) \mathcal{G}_R^8 – 8-times unfolding of \mathcal{G}_R . (c) Common transition table of even forward zigzag automata. (d) a run of the zigzag automaton over a path in \mathcal{G}_R^8 . Indices of the initial control state $I_{2,4}^{ef}$ indicate that the run encodes a path from $x_2^{(0)}$ to $x_4^{(0)}$.

Example 6. Consider the set of variables $\mathbf{x} = \{x_1, \dots, x_4\}$ and a difference bounds relation $R(\mathbf{x}, \mathbf{x}') \equiv x_2 - x'_1 \leq -1 \wedge x_3 - x'_2 \leq 0 \wedge x_1 - x'_3 \leq 0 \wedge x'_4 - x_4 \leq 0 \wedge x'_3 - x_4 \leq 0$. The graph representation \mathcal{G}_R of the relation $R(\mathbf{x}, \mathbf{x}')$ is depicted in Figure 6 (a). Figure 6 (b) shows \mathcal{G}_R^8 , the 8-times unfolding of \mathcal{G}_R . The transition table that is common to all even forward zigzag automata is given in Figure 6 (c). An example of a run of \mathcal{A}_R^{ef} recognizing a path of constraints in \mathcal{G}_R^8 is given in Figure 6 (d). The word accepted by π is a subgraph of \mathcal{G}_R^8 shown in Figure 6 (b). The cycle $\lambda: q_1 \xrightarrow{G_1} q_2 \xrightarrow{G_2} q_3 \xrightarrow{G_3} q_1$ is taken twice in this run. The weights of the symbols on the run are $w(G_1) = w(G_2) = w(G_4) = 0$ and $w(G_3) = -1$. \square

The following lemma gives several equivalent conditions for checking that an octagonal relation is well-founded. They will later be used to design an efficient polynomial time algorithm that computes the weakest recurrent set of an octagonal relation. These conditions

also provide basis for the proof of existence of linear ranking functions for well-founded octagonal relations which we give in the next section.

Lemma 7. Let $R(\mathbf{x}, \mathbf{x}')$, $\mathbf{x} = \{x_1, \dots, x_N\}$, be a $*$ -consistent octagonal relation with prefix b and $\overline{R}(\mathbf{y}, \mathbf{y}')$, $\mathbf{y} = \{y_1, \dots, y_{2N}\}$, be the difference bounds encoding of $R(\mathbf{x}, \mathbf{x}')$. Then, the following statements are equivalent.

- (1) R is well-founded
- (2) $R^{-n_1}(\mathbb{Z}^N) \neq R^{-n_2}(\mathbb{Z}^N)$ for some $n_2 > n_1 \geq b$
- (3) $R^{-n_1}(\mathbb{Z}^N) \neq R^{-n_2}(\mathbb{Z}^N)$ for some $n_2 > n_1 \geq 5^{2N}$
- (4) there exists a path $\sigma.\lambda.\sigma'$ in \mathcal{A}_R^{ef} of the form $I_{i,j}^{ef} \xrightarrow{\sigma} q \xrightarrow{\lambda} q \xrightarrow{\sigma'} F^{ef}$ for some $1 \leq i, j \leq 2N$ and a control state q such that $w(\lambda) < 0$.
- (5) \overline{R} is well-founded

Proof. (1 \Rightarrow 2) For a proof by contraposition, suppose that $R^{-n_1}(\mathbb{Z}^N) = R^{-n_2}(\mathbb{Z}^N)$ for all $n_2 > n_1 \geq b$. Thus, $R^{-b-1}(\mathbb{Z}^N) = R^{-b}(\mathbb{Z}^N)$ and consequently, $\text{wrs}(R) = R^{-b}(\mathbb{Z}^N)$, by Lemma 3. Since R is $*$ -consistent, then clearly $R^{-b}(\mathbb{Z}^N) \neq \emptyset$. Combining the above, we infer that $\text{wrs}(R) = R^{-b}(\mathbb{Z}^N) \neq \emptyset$. Thus, $\text{wrs}(R) \neq \emptyset$ and R is not well-founded, contradiction.

(1 \Rightarrow 3) Similar to (1 \Rightarrow 2).

(2 \Rightarrow 1) For a proof by contraposition, suppose that R is not well-founded. By Lemma 6, $\text{wrs}(R) = R^{-b}(\mathbb{Z}^N)$. Since $\text{wrs}(R)$ is the greatest fixpoint of pre_R , then clearly $\text{wrs}(R) = R^{-b}(\mathbb{Z}^N) = R^{-n}(\mathbb{Z}^N)$ for all $n \geq b$. Consequently, $R^{-n_1}(\mathbb{Z}^N) = \text{wrs}(R) = R^{-n_2}(\mathbb{Z}^N)$ for all $n_2 > n_1 \geq b$.

(3 \Rightarrow 4) $R^{-n_1}(\mathbb{Z}^N) \neq R^{-n_2}(\mathbb{Z}^N)$. Let $n_2 > n_1 \geq 5^{2N}$ such that $R^{-n_1}(\mathbb{Z}^N) \neq R^{-n_2}(\mathbb{Z}^N)$. Then, $\overline{R}^{-n_1}(\mathbb{Z}^{2N}) \neq \overline{R}^{-n_2}(\mathbb{Z}^{2N})$ too by contraposition: For all $m \geq 0$, the tightly closed difference bounds encoding of $R^{-m}(\mathbb{Z}^N)$ is $(M_{\overline{R}^m}^t)_{\downarrow \mathbf{y}}$, a restriction of $M_{\overline{R}^m}^t$ to the entries corresponding to unprimed variables. If $\overline{R}^{-n_1}(\mathbb{Z}^{2N}) = \overline{R}^{-n_2}(\mathbb{Z}^{2N})$, then $(M_{\overline{R}^{n_1}}^*)_{\downarrow \mathbf{y}} = (M_{\overline{R}^{n_2}}^*)_{\downarrow \mathbf{y}}$, by Proposition 2. This implies that $(M_{\overline{R}^{n_1}}^t)_{\downarrow \mathbf{y}} = (M_{\overline{R}^{n_2}}^t)_{\downarrow \mathbf{y}}$, by Theorem 2. Consequently, $R^{-n_1}(\mathbb{Z}^N) = R^{-n_2}(\mathbb{Z}^N)$, since $(M_{\overline{R}^{n_j}}^t)_{\downarrow \mathbf{y}}$ are the tight DBM representations of $R^{-n_j}(\mathbb{Z}^N)$, $j = 1, 2$.

Since $\overline{R}^{-n_1}(\mathbb{Z}^{2N}) \neq \overline{R}^{-n_2}(\mathbb{Z}^{2N})$, then $\overline{R}^{-n_1}(\mathbb{Z}^{2N}) \supset \overline{R}^{-n_2}(\mathbb{Z}^{2N})$, by monotonicity of pre_R . Consequently, $(M_{\overline{R}^{n_1}}^*)_{i,j} > (M_{\overline{R}^{n_2}}^*)_{i,j}$ for some $1 \leq i \neq j \leq 2N$, by Proposition 2. By Proposition 4, there exists a path π in $Z_{\overline{R}}$ from $I_{i,j}^{ef}$ to F^{ef} such that $w(\pi) = (M_{\overline{R}^{n_1}}^*)_{i,j}$. Moreover π has length $n_1 + 2$ and can be written as $\pi = I_{i,j}^{ef} \xrightarrow{\epsilon} q \xrightarrow{\sigma} q' \xrightarrow{\epsilon} F^{ef} \xrightarrow{\epsilon^*} F^{ef}$ where $w(\pi) = w(\sigma)$. Similarly, there is a path π' from $I_{i,j}^{ef}$ to F^{ef} of length $n_2 + 2$ such that $w(\pi') = (M_{\overline{R}^{n_2}}^*)_{i,j}$ and $\pi' = I_{i,j}^{ef} \xrightarrow{\epsilon} q \xrightarrow{\sigma'} q' \xrightarrow{\epsilon} F^{ef} \xrightarrow{\epsilon^*} F^{ef}$ where $w(\pi') = w(\sigma')$.

We prove that $|\sigma'| > n_1$ by contradiction. Suppose that $|\sigma'| \leq n_1$ and denote $n = |\sigma'|$. The path $\theta = I_{i,j}^{ef} \xrightarrow{\epsilon} q \xrightarrow{\sigma} q' \xrightarrow{\epsilon} F^{ef}$ $(M_{\overline{R}^n}^*)_{i,j} \leq w(\theta)$, by Proposition 4. We obtain that $(M_{\overline{R}^n}^*)_{i,j} \leq w(\pi') = (M_{\overline{R}^{n_2}}^*)_{i,j}$, by the fact that $w(\theta) = w(\sigma') = w(\pi')$ and by Proposition 4. Since $n \leq n_1 < n_2$, we infer that $(M_{\overline{R}^n}^*)_{i,j} = (M_{\overline{R}^{n_1}}^*)_{i,j} = (M_{\overline{R}^{n_2}}^*)_{i,j}$, by monotonicity of pre_R . Contradiction with $(M_{\overline{R}^{n_1}}^*)_{i,j} > (M_{\overline{R}^{n_2}}^*)_{i,j}$.

Since $|\sigma'| > n_1 \geq 5^{2N}$, there are cycles (at least one) in σ' . Observe that:

- None of these cycles can be positive, since positive weight would imply that π' is not a minimal run of length n_2 , which contradicts the assumption.
- Not all these cycles are zero-weight, which can be demonstrated by contradiction. Suppose all cycles are zero-weight, erase all of them from σ' and denote the resulting path ρ and its length $n = |\rho| \leq 5^{2N}$. Next, build $\theta = \sigma'_1 \cdot \rho \cdot \sigma'_3$. We infer that $(M_{\bar{R}^n}^*)_{i,j} \leq w(\pi') = (M_{\bar{R}^{n_2}}^*)_{i,j}$, since $w(\theta) = w(\rho) = w(\sigma') = w(\pi')$ and by Proposition 4. Since $n \leq n_1 < n_2$, we infer that $(M_{\bar{R}^n}^*)_{i,j} = (M_{\bar{R}^{n_1}}^*)_{i,j} = (M_{\bar{R}^{n_2}}^*)_{i,j}$, by monotonicity of pre_R . Contradiction with $(M_{\bar{R}^{n_1}}^*)_{i,j} > (M_{\bar{R}^{n_2}}^*)_{i,j}$.

The above proves that there exists at least one negative-weight cycle in σ' . Consequently, π' can be split into $\pi' = \sigma \cdot \lambda \cdot \sigma'$ where λ is a negative weight cycle.

(4 \Rightarrow 5) By Proposition 4, the length of $\sigma \cdot \sigma'$ is $|\sigma \cdot \sigma'| = m + 2$ for some $m \geq 0$ and $\sigma \cdot \sigma'$ starts in $I_{i,j}^{ef}$ and ends in F^{ef} for some $1 \leq i, j \leq 2N$. Let $p = |\lambda|$. Clearly, $(M_{\bar{R}^{m+kp}}^*)_{i,j} \leq w(\sigma \cdot \lambda^k \cdot \sigma')$ for all $k \geq 0$, by Proposition 4. The infinite sequence $\{w(\sigma \cdot \lambda^k \cdot \sigma')\}_{k \geq 0}$ is strictly decreasing and thus $\inf\{w(\sigma \cdot \lambda^k \cdot \sigma')\}_{k \geq 0} = -\infty$. Consequently $\inf\{(M_{\bar{R}^{m+kp}}^*)_{i,j}\}_{k \geq 0} = -\infty$ too. By monotonicity of pre_R ,

$$\inf\{(M_{\bar{R}^m}^*)_{i,j}\}_{m \geq 0} = \inf\{(M_{\bar{R}^{m+kp}}^*)_{i,j}\}_{k \geq 0}.$$

Thus, $\inf\{(M_{\bar{R}^m}^*)_{i,j}\}_{m \geq 0} = -\infty$. Consequently, $\text{wrs}(\bar{R}) = \bigcap_{m \geq 0} \bar{R}^{-m}(\mathbb{Z}^N) = \emptyset$ and \bar{R} is well-founded.

(5 \Rightarrow 1) If \bar{R} is well-founded, then $\bigcap_{m \geq 0} \bar{R}^{-m}(\mathbb{Z}^N) = \emptyset$. Thus, there exist $1 \leq i, j \leq N$ such that $\inf\{(M_{\bar{R}^m}^*)_{i,j}\}_{m \geq 0} = -\infty$. Since $(M_{\bar{R}^m}^t)_{i,j} \leq (M_{\bar{R}^m}^*)_{i,j}$ for all $m \geq 0$, by Theorem 2, we infer that $\inf\{(M_{\bar{R}^m}^t)_{i,j}\}_{m \geq 0} = -\infty$ too. Hence, $\bigcap_{m \geq 0} R^{-m}(\mathbb{Z}^N) = \emptyset$ and R is well-founded. \square

The main result of this section is the following algorithm which computes the weakest non-termination set of an octagonal relation, in time polynomial in the number of variables and logarithmic in the maximal absolute value among all coefficients of the relation.

Algorithm 1 Weakest Non-termination Set for Octagonal Relations

input An octagonal relation $R \subseteq \mathbb{Z}^x \times \mathbb{Z}^x$, over $\mathbf{x} = \{x_1, \dots, x_N\}$

output The weakest non-termination set of R

```

1: function WNT( $R$ )
2:    $V \leftarrow R$ 
3:   for all  $i \in 1, 2, \dots, 5N$  do
4:      $V \leftarrow V \circ V$ 
5:     if  $V \Leftrightarrow \text{false}$  then return  $\emptyset$ 
6:    $W \leftarrow V \circ R$ 
7:   if  $V^{-1}(\mathbb{Z}^x) = W^{-1}(\mathbb{Z}^x)$  then return  $V^{-1}(\mathbb{Z}^x)$ 
8:   elsereturn  $\emptyset$ 

```

Theorem 4. Given an octagonal relation $R \subseteq \mathbb{Z}^x \times \mathbb{Z}^x$, whose maximal absolute value among all coefficients is μ , Algorithm 1 computes $\text{wnt}(R)$ in at most $O(N^4 \cdot (\log \mu + N))$ time.

Proof. Note that for all $k_1 \geq 1$, $k_2 = 2^{\lceil \log_2 k_1 \rceil}$, R^{k_2} can be computed in $\lceil \log_2 k_1 \rceil$ time by iterating the assignment $R \leftarrow R \circ R$. Observe that $5N \geq \log_2(5^{2N}) = 2 \cdot \log_2 5 \cdot n$ for all $n \geq 1$. Thus, $2^{5N} \geq 5^{2N}$ for all $n \geq 1$. Notice that after executing line 6, $V \equiv R^{n_1}$, $W \equiv R^{n_2}$, where $n_1 = 2^{5N}$ and $n_2 = 2^{5N} + 1$. Clearly, $n_2 > n_1 \geq 5^{2N}$.

Consider first the case when R is $*$ -consistent. If the test on line 7 succeeds, then $V^{-1} = R^{-n_1} = \text{wrs}(R)$ by Lemma 3 and the algorithm returns the correct result. If the test fails, then $R^{-n_1}(\mathbb{Z}^N) \neq R^{-n_2}(\mathbb{Z}^N)$ and consequently, $\text{wrs}(R) = \emptyset$ by Lemma 7, and the algorithm returns the correct result. Second, consider the case when R is not $*$ -consistent. Then the test on line 5 will eventually pass and the algorithm correctly returns \emptyset .

To evaluate the time complexity of Algorithm 1, notice that the main loop is iterated at most $5N$ times, and each iteration will apply the Floyd-Warshall algorithm for to compute the composition (and check the consistency) of (the DBM encoding) of V , which corresponds to powers R^m , for $m \leq 2^{5N}$. Since the graph unfolding $\mathcal{G}_R^{2^{5N}}$, corresponding to $R^{2^{5N}}$ has $N \cdot 2^{5N}$ nodes, each elementary path in this graph is of length at most $N \cdot 2^{5N}$. Hence the maximum absolute value among the coefficients of V , at any iteration, is bounded by $\mu_{\max} = \mu \cdot N \cdot 2^{5N}$. Moreover, any run of the Floyd-Warshall algorithm for V takes at most $\mathcal{O}(N^3 \cdot \log(\mu_{\max} \cdot N)) = \mathcal{O}(N^3 \cdot (\log \mu + N))$ time. Hence the overall time complexity is at most $\mathcal{O}(N^4 \cdot (\log \mu + N))$. \square

4.6. On the Existence of Linear Ranking Functions. A ranking function for a given relation R constitutes a proof of the fact that R is well-founded. We distinguish here two cases. If R is not $*$ -consistent, then the well-foundedness of R is witnessed simply by an integer constant $i > 0$ such that $R^i = \emptyset$. Otherwise, if R is $*$ -consistent, we need a better argument for well-foundedness. In this section, we show that for any $*$ -consistent well-founded octagonal relation $R(\mathbf{x}, \mathbf{x}')$, $\mathbf{x} = \{x_1, \dots, x_N\}$, with prefix b , the (strengthened) relation defined by $(\exists \mathbf{x}'. R^B) \wedge R$, where $B = \min\{b, 5^{2N}\}$ is well-founded and has a linear ranking function even when R alone does not have one.

Definition 14. Given a relation defined by $R(\mathbf{x}, \mathbf{x}')$, a *linear ranking function* for R is a term $f(\mathbf{x}) = \sum_{i=1}^n a_i x_i$ such that for all valuations $\nu, \nu' : \mathbf{x} \rightarrow \mathbb{Z}$:

- (1) f is *decreasing*: if $\nu, \nu' \models R(\mathbf{x}, \mathbf{x}')$, then $f(\nu) > f(\nu')$,
- (2) f is *bounded*: if $\nu, \nu' \models R(\mathbf{x}, \mathbf{x}')$, then $f(\nu) > h$ and $f(\nu') > h$ for some $h \in \mathbb{Z}$.

The main result of this section is the following:

Theorem 5. Let $R(\mathbf{x}, \mathbf{x}')$ be a $*$ -consistent octagonal relation, with prefix $b \geq 0$. Then, letting $B = \min\{b, 5^{2N}\}$, R is well-founded if and only if the relation defined by $(\exists \mathbf{x}'. R^B) \wedge R$ is well founded if and only if $(\exists \mathbf{x}'. R^B) \wedge R$ has a linear ranking function.

The first part of the theorem is proved by the following lemma:

Lemma 8. Let $R(\mathbf{x}, \mathbf{x}')$ be a relation, and $m > 0$ be an integer. Then $\text{wrs}(R) = \emptyset$ if and only if $\text{wrs}(R_m) = \emptyset$, where R_m is the relation defined by $(\exists \mathbf{x}'. R^m) \wedge R$.

Proof. “ \Rightarrow ” By the fact that $R \Leftarrow (\exists \mathbf{x}'. R^m) \wedge R$ and the monotonicity of wrs . “ \Leftarrow ” We prove the dual. Assume that $\text{wrs}(R) \neq \emptyset$ i.e., there exists an infinite sequence of valuations $\sigma = \{\nu : \mathbf{x} \rightarrow \mathbb{Z}\}_{i \geq 0}$ such that $(\nu_i(\mathbf{x}), \nu_{i+1}(\mathbf{x})) \in R$, for all $i \geq 0$. Then all $\nu_i(\mathbf{x})$ belong to the set defined by $\exists \mathbf{x}'. R^m$, hence σ is an infinite sequence for the relation defined by $(\exists \mathbf{x}'. R^m) \wedge R$ as well. \square

It remains to prove that the witness relation defined by $(\exists \mathbf{x}'. R^B) \wedge R$ has a linear ranking function, provided that it is well-founded. The proof is organized as follows. We first prove the existence of such function for difference bounds relations. By Lemma 7, if the difference bounds relation R is well-founded, then the zigzag automaton Z_R must have a cycle of negative weight. Lemma 9 and 11 use the structure of this cycle, representing several of the constraints in R , to show the existence of the linear ranking function for the witness relation $(\exists \mathbf{x}'. R^B) \wedge R$. Second, using the result of Lemma 7 on equivalence of well-foundedness of an octagon R and its difference bounds representation \overline{R} , we prove the existence of linear ranking function for octagonal relations in Lemma 12.

4.6.1. Linear Ranking Function for Difference Bounds Relation. We first prove the existence of a linear decreasing function, based on the existence of a negative weight cycle in the zigzag automaton.

Lemma 9. Let $R(\mathbf{x}, \mathbf{x}')$, $\mathbf{x} = \{x_1, \dots, x_N\}$ be a $*$ -consistent and well-founded difference bounds relation with prefix $b \geq 0$. Then, there exists a linear function $f(\mathbf{x})$ such that for all valuations $\nu : \mathbf{x} \rightarrow \mathbb{Z}, \nu' : \mathbf{x}' \rightarrow \mathbb{Z}$ satisfying $\nu, \nu' \models R(\mathbf{x}, \mathbf{x}')$, we have $f(s) > f(s')$.

Proof. By Lemma 7, there exists a path $\sigma.\lambda.\sigma'$ in $Z_{\overline{R}}$ of the form $I_{i,j}^{ef} \xrightarrow{\sigma} q_1 \xrightarrow{\lambda} q_1 \xrightarrow{\sigma'} F^{ef}$ for some $1 \leq i, j \leq 2N$ and a control state q_1 such that $w(\lambda) < 0$. Let denote the length of λ by p and let write λ as $\lambda = q_1 \xrightarrow{G_1} q_2 \dots q_p \xrightarrow{G_p} q_1$. Let $G_j = (\mathbf{x} \cup \mathbf{x}', E_j)$ for all $1 \leq j \leq p$.

Consider the following sum of all constraints represented by edges appearing in the zigzag cycle (note that the sum of weights of these edges equals $w(\lambda)$):

$$\sum_{1 \leq j \leq p} \left(\sum_{(x_i \rightarrow x'_j) \in E_j} (x_i - x'_j) + \sum_{(x'_i \rightarrow x_j) \in E_j} (x'_i - x_j) \right) \leq w(\lambda) \quad (4.5)$$

The left-hand side of (4.5) can be written equivalently as

$$\sum_{1 \leq j \leq p} \left(\sum_{\substack{1 \leq i \leq n, \\ (q_j)_i = r}} (x_i - x'_i) + \sum_{\substack{1 \leq i \leq n, \\ (q_j)_i = l}} (-x_i + x'_i) + \sum_{\substack{1 \leq i \leq n, \\ (q_j)_i = lr}} (-x_i + x_i) + \sum_{\substack{1 \leq i \leq n, \\ (q_j)_i = rl}} (-x'_i + x'_i) \right) \quad (4.6)$$

and thus, after simplifications ($-x_i + x_i = 0, -x'_i + x'_i = 0$), (4.5) can be written equivalently as

$$\sum_{1 \leq j \leq p} \left(\sum_{\substack{1 \leq i \leq n, \\ (q_j)_i = r}} (x_i - x'_i) + \sum_{\substack{1 \leq i \leq n, \\ (q_j)_i = l}} (-x_i + x'_i) \right) \leq w(\lambda) \quad (4.7)$$

Let f denote the negated sum of all unprimed terms in (4.6) and f' denote the sum of all primed terms in (4.6). Then, clearly $f' = f[\mathbf{x}'/\mathbf{x}]$. Thus, (4.7) can be written as

$$f' - f \leq w(\lambda) \quad (4.8)$$

Notice that since $w(\lambda) < 0$, we establish that $f' - f < 0$ hence f is strictly decreasing. Formally $f(s) > f'(s)$ for all valuations s, s' such that $s, s' \models R(\mathbf{x}, \mathbf{x}')$. \square

Example 7. (ctd.) We illustrate the construction of linear decreasing function. R is well-founded and by Lemma 7, there exists a path depicted in Figure 6 (d) where $w(\lambda) < 0$. We follow the construction from Lemma 9 and sum the edges in λ . We obtain $x_1 - x'_3 + x_3 - x'_2 + x_2 - x'_1 + x'_4 - x_4 + x'_4 - x_4 + x'_4 - x_4 \leq -1$, which simplifies to $x_1 + x_2 + x_3 - 3x_4 - (x'_1 + x'_2 + x'_3 - 3x_4) \leq -1$. Letting $f(\mathbf{x}) = -(x_1 + x_2 + x_3 - 3x_4)$, we have that $f(\mathbf{x}) > f(\mathbf{x}')$. \square

The next auxiliary lemma proves that if the difference $x_i - x_j$ is bounded in R^k for some $k \geq 1$, it is bounded in R^B too.

Lemma 10. Let $R(\mathbf{x}, \mathbf{x}')$, $\mathbf{x} = \{x_1, \dots, x_N\}$ be a $*$ -consistent difference bounds relation with prefix $b \geq 0$ and period $c > 0$. Then, for any $1 \leq i, j \leq N$ and $k \geq 0$, we have $(M_{R^k}^*)_{i,j} < \infty \Rightarrow (M_{R^B}^*)_{i,j} < \infty$, where $B = \min\{b, 5^N\}$.

Proof. (Case $0 \leq k \leq B$) By monotonicity of pre_R , $(M_{R^k}^*)_{i,j} \geq (M_{R^B}^*)_{i,j}$. Thus if $(M_{R^k}^*)_{i,j} < \infty$, then clearly $(M_{R^B}^*)_{i,j} < \infty$.

(Case $B < k$ and $B = b$) Let $p = \lceil \frac{k-b}{c} \rceil$, and $k' = b + pc$. Note that $R^{k'} = \widehat{R}_{b,c}(\mathbf{x}, \mathbf{x}', \ell)[p/\ell]$, where $\widehat{R}_{b,c}(\mathbf{x}, \mathbf{x}', \ell)$ is the closed form of $\{R^{b+ci}\}_{i \geq 0}$. Since $k' \geq k$, by the same argument as for case $(1 \leq k \leq b)$, $(M_{R^{k'}}^*)_{i,j} < \infty$. Since $k' = b + pc$, then $x_i - x_j \leq a\ell + d$, where $a, d \in \mathbb{Z}$, is one of the conjuncts of the closed form $\widehat{R}_{b,c}(\mathbf{x}, \mathbf{x}', \ell)$. By definition of $\widehat{R}_{b,c}(\mathbf{x}, \mathbf{x}', \ell)$, we have $R^b \Leftrightarrow \widehat{R}_{b,c}(\mathbf{x}, \mathbf{x}', \ell)[0/\ell]$ and consequently, we have $(M_{R^b}^*)_{i,j} = a \cdot 0 + d = d < \infty$.

(Case $B < k$ and $B = 5^N$) By Proposition 4, there exists a path $\pi = \sigma_1.\sigma_2.\sigma_3.\sigma_4$ in $Z_{\overline{R}}$ of length $k+2$ such that $w(\pi) = (M_{R^k}^*)_{i,j}$. Let σ'_2 be a path obtained by erasing all cycles from σ_2 and let construct $\pi' = \sigma_1.\sigma'_2.\sigma_3$. Let $h = |\sigma'_2|$. Consequently, $(M_{R^h}^*)_{i,j} \leq w(\pi') < \infty$. Since $h \leq 5^N$, then $\infty > (M_{R^h}^*)_{i,j} \geq (M_{R^{5^N}}^*)_{i,j}$ by monotonicity of pre_R . \square

Last, we prove that the function f of Lemma 9 is bounded, concluding that it is indeed a ranking function. Since each run in the zigzag automaton recognizes a path from some x_i to some x_j , a run that repeats a cycle can be decomposed into a prefix, the cycle itself and a suffix. The recognized path may traverse the cycle several times, however each exit point from the cycle must match a subsequent entry point. These paths from the exit to the corresponding entries give us the necessary lower bound. In fact, these paths appear already on graphs \mathcal{G}_{R^i} for $i \geq B$, where b is the prefix of R and $B = \min\{b, 5^N\}$. Hence the need for a strengthened witness $(\exists \mathbf{x}'. R^B) \wedge R$, as R alone is not enough for proving boundedness of f .

Lemma 11. Let $R(\mathbf{x}, \mathbf{x}')$, $\mathbf{x} = \{x_1, \dots, x_N\}$ be a $*$ -consistent and well-founded difference bounds relation with prefix $b \geq 0$. Then, letting $B = \min\{b, 5^N\}$, there exists a linear ranking function for $(\exists \mathbf{x}'. R^B) \wedge R$.

Proof. Let f be a linear decreasing function from Lemma 9. Let $\lambda : q_1 \xrightarrow{G_1} q_2 \dots q_p \xrightarrow{G_p} q_1$ be the negative cycle used to construct f , and $q_1 \xrightarrow{\sigma'} F^{ef}$ be the suffix from Lemma 9. By construction of the zigzag automaton, for any $1 \leq j \leq p$,

$$|\{i \mid (q_j)_i = r\}| = |\{i \mid (q_j)_i = l\}|$$

It follows from (4.7) that each $(q_j)_i = r$ contributes to f with a term $-x_i$ and that each $(q_j)_i = l$ contributes to f with a term $+x_i$ and that each $(q_j)_i \notin \{r, l\}$ doesn't contribute at all. We now demonstrate that for each $1 \leq j \leq p$, there exists a bijective matching

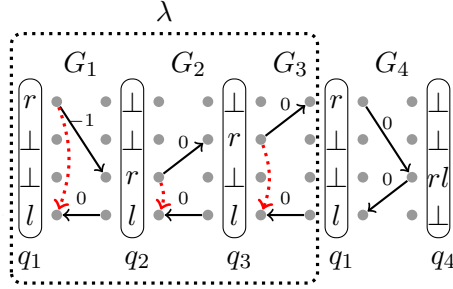


FIGURE 7. Constructing the ranking function.

$\beta_j : \{i \mid (q_j)_i = r\} \rightarrow \{i \mid (q_j)_i = l\}$ such that for any $1 \leq i_1 \leq n$ s.t. $\beta_j(i_1) = i_2$, the difference $x_{i_2} - x_{i_1}$ is bounded in $(\exists \mathbf{x}'. R^B) \wedge R$, formally $(\exists \mathbf{x}'. R^B) \wedge R \Rightarrow (x_{i_2} - x_{i_1} \geq h)$ for some $h \in \mathbb{Z}$.

Let $j \in \{1, \dots, p\}$. By construction of the zigzag automaton, the concatenated graph $G_j G_{j+1} \dots G_p \sigma'$ connects each $(q_j)_{i_1}$ s.t. $(q_j)_{i_1} = r$ with a unique $(q_j)_{i_2}$ s.t. $(q_j)_{i_2} = l$. This induces the required bijection β_j . Since $G_j G_{j+1} \dots G_p \sigma'$ is a subgraph of $\mathcal{G}_R^{p+|\sigma'|}$, it follows that there is a path $\mathbf{x}_{i_1}^{(0)} \rightsquigarrow \mathbf{x}_{i_2}^{(0)}$ in $\mathcal{G}_R^{p+|\sigma'|}$, in other words, $R^{p+|\sigma'|} \Rightarrow x_{i_1} - x_{i_2} \leq h$ for some $h \in \mathbb{Z}$. By Lemma 10, $R^B \Rightarrow x_{i_1} - x_{i_2} \leq h'$ for some $h' \in \mathbb{Z}$ too. Clearly, $(\exists \mathbf{x}'. R^B) \wedge R \Rightarrow x_{i_1} - x_{i_2} \leq h'$ too. Since $x_{i_1} - x_{i_2} \leq h'$ if and only if $x_{i_2} - x_{i_1} \geq -h'$, we obtain the required property.

Now since $f = \sum_{1 \leq j \leq p} \sum_{\substack{1 \leq i_1, i_2 \leq n \\ \beta_j(i_1) = i_2}} (x_{i_2} - x_{i_1})$ and since we proved that each of the differences $x_{i_2} - x_{i_1}$ in the sum is bounded in $(\exists \mathbf{x}'. R^B) \wedge R$, it follows that f is bounded in $(\exists \mathbf{x}'. R^B) \wedge R$ too, formally $(\exists \mathbf{x}'. R^B) \wedge R \Rightarrow (f \geq h)$ for some $h \in \mathbb{Z}$.

By Lemma 9, f is decreasing for R . Thus, f is decreasing for a stronger relation $(\exists \mathbf{x}'. R^B) \wedge R$ too, since $(\exists \mathbf{x}'. R^B) \wedge R \Rightarrow R$. Thus, f is both decreasing and bounded for $(\exists \mathbf{x}'. R^B) \wedge R$ and is a ranking function for $(\exists \mathbf{x}'. R^B) \wedge R$. \square

Example 8. (ctd.) We illustrate the boundedness of $f = -(x_1 + x_2 + x_3 - 3x_4)$ (see Figure 7). First, compute $B = \min\{b, 5^N\} = \min\{3, 5^4\} = 3$. Since there is a path $\mathbf{x}_2^{(6)} \rightsquigarrow \mathbf{x}_4^{(6)}$ in $G_3 G_4$ (and hence in \mathcal{G}_R^2), then $R^2 \Rightarrow (x_2 - x_4 \leq -1)$, and by Lemma 10, we obtain $R^B \Rightarrow (x_2 - x_4 \leq -1)$. Similarly, since there is a path $\mathbf{x}_3^{(5)} \rightsquigarrow \mathbf{x}_4^{(5)}$ in $G_2 G_3 G_4$ (and hence in \mathcal{G}_R^3), we obtain $R^B \Rightarrow (x_3 - x_4 \leq -1)$. Similarly, since there is a path $\mathbf{x}_1^{(4)} \rightsquigarrow \mathbf{x}_4^{(4)}$ in $G_1 G_2 G_3 G_4$ (and hence in \mathcal{G}_R^4), we obtain $R^B \Rightarrow (x_1 - x_4 \leq -1)$. Summing up these inequalities, we obtain that $f(\mathbf{x}) = -(x_1 + x_2 + x_3 - 3x_4) \geq 3$ and, thus $(\exists \mathbf{x}'. R^B) \wedge R \Rightarrow (f \geq 3)$.

As an experiment, we have tried the RANKFINDER [27] tool (complete for linear ranking functions), which failed to discover a ranking function on this example. This comes with no surprise, since no linear decreasing function that is bounded after the first iteration exists. However, RANKFINDER finds a ranking function for the witness relation $(\exists \mathbf{x}'. R^B) \wedge R$ instead. \square

4.6.2. Linear Ranking Functions for Octagonal Relations. In the rest of this section, let us fix the sets of variable $\mathbf{x} = \{x_1, \dots, x_N\}$ and $\mathbf{y} = \{y_1, \dots, y_{2N}\}$ for some $N \geq 1$. We first prove two technical propositions.

Proposition 5. Let $R(\mathbf{x}, \mathbf{x}')$ be a $*$ -consistent and well-founded octagonal relation, $\overline{R}(\mathbf{y}, \mathbf{y}')$ be its difference bounds encoding and let $\overline{f}(\mathbf{y})$ be a linear ranking function for $\overline{R}(\mathbf{y}, \mathbf{y}')$. Then, the function $f \stackrel{\text{def}}{=} \overline{f}[x_i/y_{2i-1}, -x_i/y_{2i}]_{i=1}^N$, is a linear ranking function for $R(\mathbf{x}, \mathbf{x}')$.

Proof. If \overline{f} is decreasing, then $\overline{f}(\overline{\mathbf{v}}) > \overline{f}(\overline{\mathbf{v}}')$ for each $(\overline{\mathbf{v}}, \overline{\mathbf{v}}') \models \overline{R}(\mathbf{y}, \mathbf{y}')$ where $\overline{\mathbf{v}}, \overline{\mathbf{v}}'$ are valuations of the form

$$\overline{\mathbf{v}} = (v_1, -v_1, \dots, v_N, -v_N), \quad \overline{\mathbf{v}}' = (v'_1, -v'_1, \dots, v'_N, -v'_N).$$

Recall that by Equation (4.2),

$$\phi(\mathbf{x}) \Leftrightarrow (\exists y_2, y_4, \dots, y_{2N} \cdot \overline{\phi} \wedge \bigwedge_{i=1}^N y_{2i-1} = -y_{2i}) [x_i/y_{2i-1}]_{i=1}^N$$

for each octagonal constraint ϕ . Defining $f \stackrel{\text{def}}{=} \overline{f}[x_i/y_{2i-1}, -x_i/y_{2i}]_{i=1}^N$, it follows by the above observations that $f(\mathbf{v}) > f(\mathbf{v}')$ for each $(\mathbf{v}, \mathbf{v}') \models R(\mathbf{x}, \mathbf{x}')$. Hence, f is decreasing too. Similarly, we can prove that f is bounded as well. Since f is clearly linear by definition, it follows that it is a linear ranking function for $R(\mathbf{x}, \mathbf{x}')$. \square

Proposition 6. Let $R(\mathbf{x}, \mathbf{x}')$ be a $*$ -consistent and well-founded octagonal relation, $\overline{R}(\mathbf{y}, \mathbf{y}')$ be its difference bounds encoding and let $\overline{f}(\mathbf{y})$ be a linear ranking function for $(\exists \mathbf{y}'. \overline{R}^m) \wedge \overline{R}$, $m \geq 0$. Then, $f \stackrel{\text{def}}{=} \overline{f}[x_i/y_{2i-1}, -x_i/y_{2i}]_{i=1}^N$ is a linear ranking function for $(\exists \mathbf{x}'. R^m) \wedge R$.

Proof. By the hypothesis, $\overline{f}(\mathbf{y})$ is a linear ranking function for a difference bounds relation $(\exists \mathbf{y}'. \overline{R}^m) \wedge \overline{R}$. By Proposition 5, $f(\mathbf{x})$ is a linear ranking function for $(\exists \mathbf{y}'. \overline{R}^m) \wedge \overline{R}$. Observe that

$$\begin{aligned} (\exists \mathbf{x}'. R^m) \wedge R &\Leftrightarrow \overline{(\exists \mathbf{x}'. R^m) \wedge R} && \text{(by Equation (4.1))} \\ &\Leftrightarrow \overline{(\exists \mathbf{x}'. R^m)} \wedge \overline{R} && \text{(by definition of } \overline{\phi}) \\ &\Leftrightarrow \overline{(\exists \mathbf{y}'. \overline{R}^m)} \wedge \overline{R} && \text{(by Corollary 1)} \end{aligned}$$

Thus, $f(\mathbf{x})$ is a linear ranking function for $(\exists \mathbf{x}'. R^m) \wedge R$. \square

Finally, we show that for each $*$ -consistent and well-founded octagonal relation, the corresponding witness relation has a linear ranking function, which proves the second part of Theorem 5.

Lemma 12. Let $R(\mathbf{x}, \mathbf{x}')$ be a $*$ -consistent and well-founded octagonal relation with prefix b . Then, letting $B = \min\{b, 5^{2N}\}$, there exists a linear ranking function for $(\exists \mathbf{x}'. R^B) \wedge R$.

Proof. By Lemma 7, $\overline{R}(\mathbf{y}, \mathbf{y}')$ is well-founded too and moreover, $\overline{R}(\mathbf{y}, \mathbf{y}')$ is $*$ -consistent by Theorem 1. Let \overline{b} be the prefix of \overline{R} and define $\overline{B} = \min\{\overline{b}, 5^{2N}\}$. By Lemma 11, there exists a linear ranking function \overline{f} for $(\exists \mathbf{y}'. \overline{R}^{\overline{B}}) \wedge \overline{R}$. By Proposition 6, the function $f \stackrel{\text{def}}{=} \overline{f}[x_i/y_{2i-1}, -x_i/y_{2i}]_{i=1}^N$ is a linear ranking function for $(\exists \mathbf{x}'. R^{\overline{B}}) \wedge R$. To see that f is a linear ranking function for $(\exists \mathbf{x}'. R^B) \wedge R$ too, consider arbitrary term $y_i - y_j$ considered in the proof of Lemma 11. If $b \geq \overline{b}$, then the boundedness argument ($y_i - y_j$ is bounded in R^b) follows by monotonicity of pre_R and is similar to the first case of the proof of Lemma

10. If $b < \bar{b}$, one can use a similar argument as in the second case of the proof of Lemma 10 and show, using the closed form of R instead of \bar{R} , that $y_i - y_j$ is bounded in R^b too. \square

5. LINEAR AFFINE RELATIONS

The previous section was concerned with computing weakest non-termination preconditions for non-deterministic integer relations (octagonal relations). Here, we present linear affine relations which are a general model of deterministic transition relations. Linear affine relations are conjunctions of equalities of the form $x' = a_1x_1 + \dots + a_nx_n + b$, where $a_1, \dots, a_n \in \mathbb{Z}$ are integer coefficients, and Presburger definable conditions on the unprimed variables x_1, \dots, x_n . First, we show that the weakest recurrent set of a linear affine relation R can be computed as the limit of a descending Kleene sequence $\mathbb{Z}^x \supseteq \text{pre}_R(\mathbb{Z}^x) \supseteq \text{pre}_R^2(\mathbb{Z}^x) \supseteq \dots$. Second, this set can be defined in Presburger arithmetic for a subclass of affine relations with the *finite monoid property* (Section 5.3). Finally, we relax the finite monoid condition and describe a method for generating sufficient termination conditions, i.e. sets $S \in \mathbb{Z}^n$ such that $S \cap \text{wrs}(R) = \emptyset$, for the class of *polynomially bounded* affine relations (Section 5.4).

Definition 15. Let $\mathbf{x} = \langle x_1, \dots, x_N \rangle$ be a vector of variables ranging over \mathbb{Z} . A relation $R \in \mathbb{Z}^N \times \mathbb{Z}^N$ is an *affine relation* if it can be defined by a formula $R(\mathbf{x}, \mathbf{x}')$ of the form

$$R(\mathbf{x}, \mathbf{x}') \Leftrightarrow \mathbf{x}' = A \times \mathbf{x} + \mathbf{b} \wedge \phi(\mathbf{x}) \quad (5.1)$$

where $A \in \mathbb{Z}^{N \times N}$, $\mathbf{b} \in \mathbb{Z}^N$, and ϕ is a Presburger formula over unprimed variables only, called the *guard*. The formula $\mathbf{x}' = A \times \mathbf{x} + \mathbf{b}$, defining a linear transformation, is called the *update*.

5.1. Background on Linear Algebra. We first recall several notions of linear algebra, needed in the following. A complex number r is said to be a *root of the unity* if $r^d = 1$ for some integer $d > 0$. If $A \in \mathbb{Z}^{n \times n}$ is a square matrix, and $\mathbf{v} \in \mathbb{Z}^n$ is a column vector of integer constants, then any complex number $\lambda \in \mathbb{C}$ such that $A\mathbf{v} = \lambda\mathbf{v}$, for some complex vector $\mathbf{v} \in \mathbb{C}^n$, is called an *eigenvalue* of A . The vector \mathbf{v} in this case is called an *eigenvector* of A . It is known that the eigenvalues of A are the roots of the *characteristic polynomial* $P_A(x) = \det(A - xI_n) = 0$, which is an effectively computable univariate polynomial. The *minimal polynomial* of A is the polynomial μ_A of lowest degree such that $\mu_A(A) = 0$. By the Cayley-Hamilton Theorem, the minimal polynomial always divides the characteristic polynomial, i.e. the roots of the former are root of the latter.

If $\lambda_1, \dots, \lambda_m$ are the eigenvalues of A , then $\lambda_1^p, \dots, \lambda_m^p$ are the eigenvalues of A^p , for all integers $p > 0$. A matrix is said to be *diagonalizable* if and only if there exists a non-singular matrix $U \in \mathbb{C}^{N \times N}$ and a diagonal matrix with the eigenvalues $\lambda_1, \dots, \lambda_m$ occurring on the main diagonal, such that $A = U \times D \times U^{-1}$. This is the case if and only if μ_A has only roots of multiplicity one³.

³See e.g. Thm 8.47 in [5].

5.2. Termination Preconditions for Deterministic Relations. First, we show that the pre-image function of a deterministic relation is \cap -continuous. Since affine transformations are deterministic, this means that their weakest non-termination preconditions can be computed as limits of descending Kleene sequences. Let \mathbf{x} be a set of variables in the following.

Lemma 13. Let $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ be a deterministic relation. Then, pre_R is \cap -continuous.

Proof. Let $I = \{1, \dots, d\}$, $d \in \mathbb{N}_\infty$, and $\{S_i \subseteq \mathbb{Z}^{\mathbf{x}}\}_{i \in I}$ be a potentially infinite collection of sets. We prove that:

$$\text{pre}_R(\bigcap_{i \in I} S_i) = \bigcap_{i \in I} \text{pre}_R(S_i).$$

“ \Rightarrow ” By monotonicity of pre_R , we have $\text{pre}_R(\bigcap_{i \in I} S_i) \subseteq \text{pre}_R(S_i)$ for all $i \in I$ and hence, $\text{pre}_R(\bigcap_{i \in I} S_i) \subseteq \bigcap_{i \in I} \text{pre}_R(S_i)$. “ \Leftarrow ” Let $v \in \bigcap_{i \in I} \text{pre}_R(S_i)$. Then, there exists $v_i \in S_i$ such that $(v, v_i) \in R$ for all $i \in I$. Since R is deterministic, then $v_1 = v_i$ for all $i \in I$ and hence $v_1 \in \bigcap_{i \in I} S_i$. Consequently, $v \in \text{pre}_R(\bigcap_{i \in I} S_i)$. \square

Second, we prove that the closed form of a deterministic relation can be defined in Presburger arithmetic whenever the closed form of its update can be defined in Presburger arithmetic. Concretely, the (logical definition of) a deterministic relation R can be split into a guard and a deterministic update, and the closed form of R can be computed based on the closed form of the update.

Lemma 14. Let $R \subseteq \mathbb{Z}^{\mathbf{x}} \times \mathbb{Z}^{\mathbf{x}}$ be a $*$ -consistent deterministic relation and $\varphi(\mathbf{x})$ be a guard. Then the transitive closure of the relation $R \wedge \varphi$ can be defined as:

$$(R \wedge \varphi)^+(\mathbf{x}, \mathbf{x}') \Leftrightarrow \exists k > 0 . \widehat{R}(k, \mathbf{x}, \mathbf{x}') \wedge \forall 0 \leq \ell < k \exists \mathbf{y} . \widehat{R}(\ell, \mathbf{x}, \mathbf{y}) \wedge \varphi(\mathbf{y})$$

where \widehat{R} defines the closed form of R .

Proof. “ \Rightarrow ” Let $\nu, \nu' \in \mathbb{Z}^{\mathbf{x}}$ be a pair of valuations, such that $\nu, \nu' \models (R \wedge \varphi)^+$. Then there exists $n > 0$ such that $\nu, \nu' \models (R \wedge \varphi)^n$. Consequently, there exists a sequence of valuations $\nu = \nu_0, \nu_1, \dots, \nu_n = \nu' \in \mathbb{Z}^{\mathbf{x}}$, such that $\nu_i, \nu_{i+1} \models R \wedge \varphi$. By Definition 4, we have that $\models \widehat{R}(n, \nu_0, \nu_n)$ and $\models \widehat{R}(i, \nu_0, \nu_i) \wedge \varphi(\nu_i)$, for all $i = 0, \dots, n-1$.

“ \Leftarrow ” Let $\nu, \nu' \in \mathbb{Z}^{\mathbf{x}}$ be two valuations such that $\models \widehat{R}(n, \nu, \nu')$ for some $n > 0$ and for all $i = 0, \dots, n-1$ we have $\models \widehat{R}(i, \nu, \nu_i)$ and $\models \varphi(\nu_i)$, for some valuation ν_i of \mathbf{x} . Since $\widehat{R}(n) \Leftrightarrow R^n$, by Definition 4, there exists a sequence of valuations $\nu = \nu'_0, \nu'_1, \dots, \nu'_n = \nu' \in \mathbb{Z}^{\mathbf{x}}$ such that $\nu'_i, \nu'_{i+1} \models R$. By the fact that R was assumed to be deterministic, we have $\nu_i = \nu'_i$ for all $i = 0, \dots, n-1$, hence $\nu'_i \models \varphi$, for all $i = 0, \dots, n-1$. Clearly then $\nu, \nu' \models (R \wedge \varphi)^+$. \square

Since linear affine relations are deterministic, the weakest recurrent set of arbitrary linear affine relation R can be computed as $\text{wrs}(R) = \bigcap_{m \geq 0} \text{pre}_R^m(\mathbb{Z}^N)$, by Lemma 13 and Lemma 3. Hence, the weakest recurrent set can be defined using the closed form of R :

$$\text{wrs}(R) \equiv \forall k \geq 0 . \exists \mathbf{x}' . \widehat{R}(\mathbf{x}, \mathbf{x}', k)$$

By defining R as $R_u(\mathbf{x}, \mathbf{x}') \wedge \phi(\mathbf{x})$ where $R_u(\mathbf{x}, \mathbf{x}')$ is a deterministic update and $\phi(\mathbf{x})$ is a Presburger guard, we can write the closed form of R , by Lemma 14, as

$$\widehat{R}(k, \mathbf{x}, \mathbf{x}') \Leftrightarrow \widehat{R}_u(k, \mathbf{x}, \mathbf{x}') \wedge \forall 0 \leq \ell < k \exists \mathbf{y} . \widehat{R}_u(\ell, \mathbf{x}, \mathbf{y}) \wedge \varphi(\mathbf{y})$$

Then, the definition of the weakest recurrent set of a linear affine relation is (after the elimination of the trailing existential quantifier and renaming ℓ with k and \mathbf{y} with \mathbf{x}'):

$$\text{wrs}(R)(\mathbf{x}) \equiv \forall k \geq 0 . \exists \mathbf{x}' . \widehat{R}_u(k, \mathbf{x}, \mathbf{x}') \wedge \varphi(\mathbf{x}') \quad (5.2)$$

5.3. Finite Monoid Affine Relations. The class of finite monoid affine relations was the first class of integer relations for which the transitive closure has been shown to be Presburger definable, by Boigelot [5]. Informally, an affine relation is a finite monoid relation if the set of powers of its transformation matrix is finite. Originally, Boigelot characterized this class by two decidable conditions in [5] (we report on these conditions in Lemma 6). Later, Finkel and Leroux noticed in [18] that Boigelot's conditions correspond to the finite monoid property, which is also known to be decidable [24].

Given a vector $\mathbf{x} = \langle x_1, \dots, x_N \rangle$ of variables, an affine transformation

$$R(\mathbf{x}, \mathbf{x}') \Leftrightarrow \mathbf{x}' = A \times \mathbf{x} + \mathbf{b} \wedge \phi(\mathbf{x})$$

where $A \in \mathbb{Z}^{N \times N}$, $\mathbf{b} \in \mathbb{Z}^N$, is said to have the *finite monoid property* [5, 18] if the monoid of powers of A , denoted as $\langle \mathcal{M}_A, \times \rangle$, where $\mathcal{M}_A = \{A^i \mid i \geq 0\}$, is finite. Here $A^0 = I_N$ and $A^i = A \times A^{i-1}$, for $i > 0$. It has been shown in [18] that finite monoid property can be equivalently characterized by the following two conditions.

Theorem 6. [[5], [18]] An affine transformation $R \equiv A \times \mathbf{x} + \mathbf{b}$, where $A \in \mathbb{Z}^{N \times N}$ and $\mathbf{b} \in \mathbb{Z}^N$ has the finite monoid condition if and only if there exists $p > 0$ such that the following hold:

- (1) every eigenvalue of A^p belongs to the set $\{0, 1\}$,
- (2) the minimal polynomial $\mu_{A^p}(x)$ of A^p belongs to the set $\{0, x, x-1, x(x-1)\}$ (or, equivalently, A^p is diagonalizable).

Both conditions in the above theorem are decidable [5, 24]. It was shown in [5, 18, 8] that the closed form of (the update part of) a linear affine transformation with the finite monoid property is Presburger definable. This entails the decidability of the universal termination problem for finite monoid affine relations.

Theorem 7. The weakest non-termination precondition of a finite monoid affine relation is Presburger definable and effectively computable. Consequently, the termination problem is decidable for finite monoid affine relations.

5.4. Polynomially Bounded Affine Relations. In the following, we study another subclass of affine relations with linear guards and transformation matrices whose eigenvalues are either zero or roots of the unity.

Definition 16. If $\mathbf{x} = \langle x_1, \dots, x_N \rangle$ is a vector of variables ranging over \mathbb{Z} , a *polynomially bounded affine relation* is a relation of the form

$$R(\mathbf{x}, \mathbf{x}') \Leftrightarrow \mathbf{x}' = A \times \mathbf{x} + \mathbf{b} \wedge C\mathbf{x} \geq \mathbf{d} \quad (5.3)$$

where $A \in \mathbb{Z}^{n \times n}$, $C \in \mathbb{Z}^{p \times n}$ are matrices, and $\mathbf{b} \in \mathbb{Z}^n$, $\mathbf{d} \in \mathbb{Z}^p$ are column vectors of integer constants and moreover, all eigenvalues of A are either zero or roots of the unity.

Note that, if A is a finite monoid matrix, then all eigenvalues of A are either zero or roots of the unity. Thus, the condition on A is weaker for polynomially bounded affine relations. However, since the guard of finite monoid relations is more general (Presburger), the two classes are incomparable.

The closed form of polynomially bounded affine relations cannot be defined in Presburger arithmetic any longer, thus we renounce defining $\text{wrs}(R)$ precisely, and content ourselves with the discovery of *sufficient conditions for termination*. Basically, given a linear

affine relation R , we aim at finding a disjunction $\phi(\mathbf{x})$ of linear constraints on \mathbf{x} , such that $\phi \wedge \text{wrs}(R)$ is inconsistent without explicitly computing $\text{wrs}(R)$. For this, we use several existing results from linear algebra (see, e.g., [17]). In the following, it is convenient to work with the equivalent homogeneous form:

$$R(\mathbf{x}, \mathbf{x}') \equiv C_h \mathbf{x}_h \geq \mathbf{0} \wedge \mathbf{x}'_h = A_h \mathbf{x}_h$$

$$A_h = \begin{pmatrix} a & \mathbf{b} \\ 0 & 1 \end{pmatrix} \quad C_h = \begin{pmatrix} C & -\mathbf{d} \end{pmatrix} \quad \mathbf{x}_h = \begin{pmatrix} \mathbf{x} \\ x_{N+1} \end{pmatrix} \quad (4)$$

The weakest recurrent set of R can be then defined as:

$$\text{wrs}(R) \equiv \exists x_{N+1} . \forall k \geq 0 . C_h A_h^k \mathbf{x}_h \geq \mathbf{0} \wedge x_{N+1} = 1 \quad (5.5)$$

Definition 17. A function $f : \mathbb{N} \rightarrow \mathbb{C}$ is said to be a *C-finite recurrence* if and only if:

$$f(m+d) = a_{d-1}f(m+d-1) + \dots + a_1f(m+1) + a_0f(m), \quad \forall m \geq 0$$

for some $d \in \mathbb{N}$ and $a_0, a_1, \dots, a_{d-1} \in \mathbb{C}$, with $a_{d-1} \neq 0$. The polynomial $x^d - a_{d-1}x^{d-1} - \dots - a_1x - a_0$ is called the *characteristic polynomial* of f .

A C-finite recurrence always admits a closed form.

Theorem 8 ([17]). The closed form of a C-finite recurrence is:

$$f(m) = p_1(m)\lambda_1^m + \dots + p_s(m)\lambda_s^m$$

where $\lambda_1, \dots, \lambda_s \in \mathbb{C}$ are non-zero distinct roots of the characteristic polynomial of f , and $p_1, \dots, p_s \in \mathbb{C}[m]$ are polynomials of degree less than the multiplicities of $\lambda_1, \dots, \lambda_s$, respectively.

Next, we define the closed form for the sequence of powers of A .

Corollary 2. Given a square matrix $A \in \mathbb{Z}^{N \times N}$, we have:

$$(A^m)_{i,j} = p_{1,i,j}(m)\lambda_1^m + \dots + p_{s,i,j}(m)\lambda_s^m$$

where $\lambda_1, \dots, \lambda_s \in \mathbb{C}$ are non-zero distinct eigenvalues of A , and $p_{1,i,j}, \dots, p_{s,i,j} \in \mathbb{C}[m]$ are polynomials of degree less than the multiplicities of $\lambda_1, \dots, \lambda_s$, respectively.

Proof. If $\det(A - xI_n) = x^d - a_{d-1}x^{d-1} - \dots - a_1x - a_0$ is the characteristic polynomial of A , then we have

$$A^d - a_{d-1}A^{d-1} - \dots - a_1A - a_0 = 0$$

by the Cayley-Hamilton Theorem. If we define $f_{i,j}(m) = (A^m)_{i,j}$, then we have

$$\begin{aligned} A^{m+d} &= a_{d-1}A^{m+d-1} + \dots + a_1A^{m+1} + a_0A^m \\ f_{i,j}(m+d) &= a_{d-1}f_{i,j}(m+d-1) + \dots + a_1f_{i,j}(m+1) + a_0f_{i,j}(m) \end{aligned}$$

By Theorem 8, we have that

$$(A^m)_{i,j} = p_{1,i,j}(m)\lambda_1^m + \dots + p_{s,i,j}(m)\lambda_s^m$$

for some polynomials $p_{1,i,j}, \dots, p_{s,i,j} \in \mathbb{C}[m]$ of degrees less than the multiplicities of $\lambda_1, \dots, \lambda_s$, respectively. \square

Lemma 15. Given a square matrix $A \in \mathbb{Z}^{N \times N}$, whose non-zero eigenvalues are all roots of the unity. Then $(A^m)_{i,j} \in \mathbb{Q}[m]$, for all $1 \leq i, j \leq N$, are effectively computable polynomials with rational coefficients.

Proof. Assume from now on that all non-zero eigenvalues $\lambda_1, \dots, \lambda_s$ of A are such that $\lambda_1^{d_1} = \dots = \lambda_s^{d_s} = 1$, for some integers $d_1, \dots, d_s > 0$. The method given in [5] for testing the finite monoid condition for A gives also bounds for d_1, \dots, d_s . Then we have $\lambda_1^L = \dots = \lambda_s^L = 1$, where $L = \text{lcm}(d_1, \dots, d_s)$. As d_1, \dots, d_s are effectively bounded, so is L . By Corollary 2, we have that, if m is a multiple of L , then $(A^m)_{i,j} = p_{i,j}(m)$ for some effectively computable polynomial $p_{i,j} \in \mathbb{C}[m]$ i.e., for m multiple of L , A^m is polynomially definable. But since $p_{i,j}(m)$ assumes real values in an infinity of points $m = kL$, $k > 0$, it must be that its coefficients are all real numbers, i.e. $p_{i,j} \in \mathbb{R}[m]$. Moreover, these coefficients are the solutions of the integer system:

$$\begin{cases} p_{i,j}(L) &= (A^L)_{i,j} \\ &\dots \\ p_{i,j}((d+1)L) &= (A^{(d+1)L})_{i,j} \end{cases}$$

Clearly, since $A \in \mathbb{Z}^{N \times N}$, $A^p \in \mathbb{Z}^{N \times N}$, for any $p \geq 0$. Hence $p_{i,j} \in \mathbb{Q}[m]$. \square

We turn now back to the problem of defining $\text{wrs}(R)$ for linear affine relations R of the form (5.5). First notice that, if all non-zero eigenvalues of A are roots of the unity, then the same holds for A_h (4). By Lemma 15, one can find rational polynomials $p_{i,j}(k)$ defining $(A_h^k)_{i,j}$, for all $1 \leq i, j \leq N$. The condition (5.5) resumes to a conjunction of the form:

$$\text{wrs}(R)(\mathbf{x}) \equiv \bigwedge_{i=1}^n \forall k \geq 0 . P_i(k, \mathbf{x}) \geq 0 \quad (5.6)$$

where each $P_i = a_{i,d}(\mathbf{x}) \cdot k^d + \dots + a_{i,1}(\mathbf{x}) \cdot k + a_{i,0}(\mathbf{x})$ is a polynomial in k whose coefficients are the linear combinations $a_{i,d} \in \mathbb{Q}[\mathbf{x}]$. We are looking after a sufficient condition for termination, which is, in this case, any set of valuations of \mathbf{x} that would invalidate (5.6). The following proposition gives sufficient invalidating clauses for each conjunct above. By taking the disjunction of all these clauses we obtain a sufficient termination condition for R .

Lemma 16. Given a polynomial $P(k, \mathbf{x}) = a_d(\mathbf{x}) \cdot k^d + \dots + a_1(\mathbf{x}) \cdot k + a_0(\mathbf{x})$, there exists $n > 0$ such that $P(n, \mathbf{x}) < 0$ if, for some $i = 0, 1, \dots, d$, we have $a_{d-i}(\mathbf{x}) < 0$ and $a_d(\mathbf{x}) = a_{d-1}(\mathbf{x}) = \dots = a_{d-i+1}(\mathbf{x}) = 0$.

Proof. Assuming the condition $a_{d-i}(\mathbf{x}) < 0$ and $a_d(\mathbf{x}) = a_{d-1}(\mathbf{x}) = \dots = a_{d-i+1}(\mathbf{x}) = 0$, for some $0 \leq i \leq d$, we have $P(k, \mathbf{x}) = a_{d-i}(\mathbf{x}) \cdot k^d + \dots + a_1(\mathbf{x}) \cdot k + a_0(\mathbf{x})$. Since the dominant coefficient $a_{d-i}(\mathbf{x})$ is negative, the polynomial will assume only negative values, from some point on. \square

Example 9. Consider the following program [15], and its linear transformation matrix A .

$$\begin{array}{l} \text{while } (x \geq 0) \\ \quad x' = x + y \\ \quad y' = y + z \end{array} \quad A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \quad A^k = \begin{pmatrix} 1 & k & \frac{k(k-1)}{2} \\ 0 & 1 & k \\ 0 & 0 & 1 \end{pmatrix}$$

The characteristic polynomial of A is $\det(A - \lambda I_3) = (1 - \lambda)^3$, hence the only eigenvalue is 1, with multiplicity 3. Then we compute A^k (see above), and $x' = x + k \cdot y + \frac{k(k-1)}{2} z$

gives the value of x after k iterations of the loop. Hence the (precise) non-termination condition is: $\forall k \geq 0 . \frac{z}{2} \cdot k^2 + (y - \frac{z}{2}) \cdot k + x \geq 0$. A sufficient condition for termination is: $(z < 0) \vee (z = 0 \wedge y < 0) \vee (z = 0 \wedge y = 0 \wedge x < 0)$ \square

We can generalize this method further to the case where all eigenvalues of A are of the form $q \cdot r$, with $q \in \mathbb{R}$ and $r \in \mathbb{C}$ being a root of the unity. The main reason for not using this condition from the beginning is that we are, to this point, unaware of its decidability status. With this condition instead, it is sufficient to consider only the eigenvalues with the maximal absolute value, and the polynomials obtained as sums of the polynomial coefficients of these eigenvalues. The result of Lemma 15 and the sufficient condition of Lemma 16 carry over when using these polynomials instead.

6. TERMINATION ANALYSIS OF INTEGER PROGRAMS

In this section, we extend the computation of weakest non-termination preconditions from simple conjunctive loops to programs with possibly nested loops. The method described here applies the *transition invariants* technique, initially developed for proving program termination [28], to the computation of weakest non-termination preconditions.

The method can be summarized as follows. Suppose that R is the (disjunctive) transition relation of a program. Our method first computes (1) a *transition invariant*, i.e., a relation $R_1^\# \cup \dots \cup R_m^\#$ which overapproximates the transitive closure of R restricted to states reachable from a set $Init$ of initial configurations, and (2) the *reachability relation*, defined as the restriction of the transitive closure of the transition relation R^+ to the initial program configurations $Reach = \{(s, s') \mid s \in Init, (s, s') \in R^+\}$. For computing R^+ we can use, e.g., the method described in [10]. Next, we compute the weakest non-termination set $wnt(R_i^\#)$ of each disjunct $R_i^\#$, by applying Algorithm 1. The weakest non-termination precondition of the program is then overapproximated by the pre-image of $wnt(R_1^\#) \cup \dots \cup wnt(R_m^\#)$ via its the reachability relation, i.e., $Reach^{-1}(wnt(R_1^\#) \cup \dots \cup wnt(R_m^\#))$, or equivalently, $\bigcup_{i=1}^m Reach^{-1}(wnt(R_i^\#))$.

The technique presented in this section can be further applied to programs with (recursive) procedure calls, by using the program transformation described in [3], that turns programs with recursive procedure calls into programs without procedures, with equivalent non-termination preconditions. The main ingredient of this technique is the *summarization* of procedures, i.e., computing an overapproximation of the relation between the values of the input parameters and the values returned by the procedure.

6.1. Motivation. Consider the non-deterministic integer program in Figure 8(a). If $x = 0$ initially, the program terminates immediately. It is easy to see that when $x < 0$ initially, the program can loop infinitely between lines 1 and 4. If $x > 0$ initially, the program terminates, since the tuple of valuations of $\langle x, y \rangle$ decreases (in the lexicographic order) with each iteration, and the loop can be fired only for values $x > 0$.

We view programs as control flow graphs (CFG) labeled with arithmetic formulae. Figure 8(b) depicts the control flow graph of the program in Figure 8(a).

The mechanics of our algorithm computing the weakest non-termination set applied on the above example is as follows. First, we collapse the loops in Figure 8(b) into self-loops, obtaining a reduced control flow graph in Figure 8(c). Then, we compute a *transition*

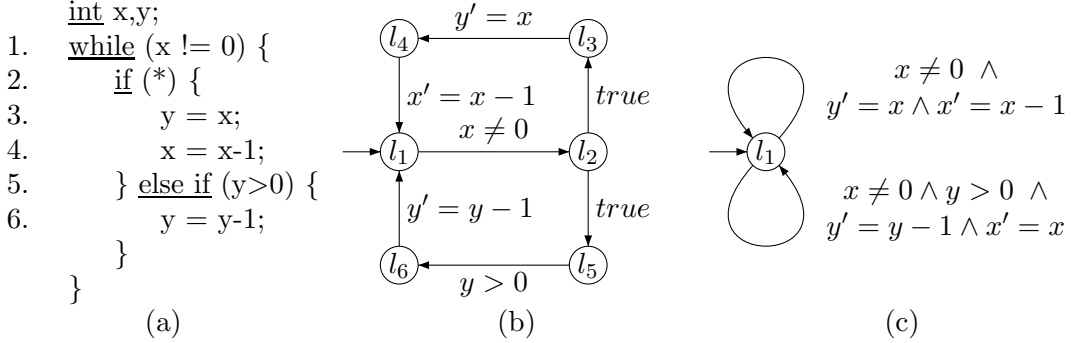


FIGURE 8. Example Program and its Control Flow Graph

invariant $TInv$ of the program $TInv \equiv R_1 \vee R_2 \vee R_3 \vee R_4 \vee R_5$, where:

$$\begin{array}{ll}
R_1 \equiv x' \geq 1 \wedge y' \geq 0 \wedge x' \leq x - 1 \wedge y' \leq x' & \text{wnt}(R_1) \equiv \perp \\
R_2 \equiv x \leq -1 \wedge y' \leq x \wedge y' = x' + 1 & \text{wnt}(R_2) \equiv x \leq -1 \\
R_3 \equiv y' \geq 1 \wedge y' \leq x \wedge y' = x' + 1 & \text{wnt}(R_3) \equiv \perp \\
R_4 \equiv x \geq 1 \wedge x' \geq 1 \wedge x' = x \wedge y' \geq 0 \wedge y' \leq y - 1 & \text{wnt}(R_4) \equiv \perp \\
R_5 \equiv x \leq -1 \wedge x' = x \wedge x' \leq -1 \wedge y' \geq 0 \wedge y' \leq y - 1 & \text{wnt}(R_5) \equiv \perp
\end{array}$$

Next, we compute the weakest non-termination set of each disjunct of $TInv$, obtaining $\text{wnt}(R_1), \dots, \text{wnt}(R_5)$ defined above. The disjunction of these non-termination set defines a set of configurations from which a non-terminating run that starts in l_1 exists:

$$\mathcal{N} \equiv \text{wnt}(R_1) \vee \text{wnt}(R_2) \vee \text{wnt}(R_3) \vee \text{wnt}(R_4) \vee \text{wnt}(R_5) \equiv x \leq -1$$

6.2. Syntax and Semantics. In the following, we abstract from specific programming language constructs and assume that programs are represented by control flow graphs (CFG) whose edges are labeled by Presburger arithmetic formulae defining relations. Formally, an *integer program* is a tuple $P = \langle \mathbf{x}, Q, q_i, \Delta \rangle$, where:

- \mathbf{x} is the set of variables of P
- Q are the *control states* of P
- Δ is a set of *transition rules* of the form $q \xrightarrow{R(\mathbf{x}, \mathbf{x}')} q'$, where $q, q' \in Q$ are the source and destination state, and $R(\mathbf{x}, \mathbf{x}')$ defines a Presburger arithmetic relation
- q_i is the *initial* control state of P

An example of an integer program is given in Figure 8(a).

A *configuration* of a program $P = \langle \mathbf{x}, Q, q_i, \Delta \rangle$ is a pair $\langle q, \nu \rangle$, where $q \in Q$ is a control state and $\nu \in \mathbb{Z}^{\mathbf{x}}$ is a valuation of the variables. Given two configurations $\langle q, \nu \rangle$ and $\langle q', \nu' \rangle$ of a program P , the configuration $\langle q', \nu' \rangle$ is said to be an *immediate successor* of $\langle q, \nu \rangle$ if and only if $q \xrightarrow{R} q' \in \Delta$ and $\nu, \nu' \models R$. A *run* of length k of the program P from q to q' is a finite sequence $\langle q_0, \nu_0 \rangle \rightarrow \langle q_1, \nu_1 \rangle \rightarrow \dots \rightarrow \langle q_k, \nu_k \rangle$, such that $q = q_0$, $q' = q_k$, and $\langle q_{i+1}, \nu_{i+1} \rangle$ is an immediate successor of $\langle q_i, \nu_i \rangle$, for all $0 \leq i < k$. An *infinite run* of a program P from a control state q is an infinite sequence $\langle q_0, \nu_0 \rangle \rightarrow \langle q_1, \nu_1 \rangle \rightarrow \dots$ such that $q = q_0$ and $\langle q_{i+1}, \nu_{i+1} \rangle$ is an immediate successor of $\langle q_i, \nu_i \rangle$ for all $i \geq 0$. We define the

transitive relation of the program as:

$$\llbracket P \rrbracket^+(q, q') \stackrel{\text{def}}{=} \{(\nu, \nu') \mid (q, \nu) \rightarrow \dots \rightarrow (q', \nu') \text{ is a run of } P \text{ of length } k \geq 1\}$$

and the *reflexive and transitive relation* $\llbracket P \rrbracket^*$ as the extension of $\llbracket P \rrbracket^+$ which considers runs of length zero as well. The *weakest non-termination set* of a program P denoted as $\llbracket P \rrbracket^{wnt}(q)$, is the set of configurations (q, ν) from which an infinite run is possible. The set of configurations with control state q , that are reachable from the initial state q_i , can be defined as the post-image of \mathbb{Z}^x via $\llbracket P \rrbracket^*(q_i, q)$. With this notation, the *transition invariant* $\llbracket P \rrbracket^{TInv}$ of a program \mathcal{P} is defined for each $q, q' \in Q$ as the restriction of the transitive relation to the set of reachable configurations:

$$\llbracket P \rrbracket^{TInv}(q, q') \stackrel{\text{def}}{=} \llbracket P \rrbracket(q, q') \wedge (\llbracket P \rrbracket^*(q_i, q))(\mathbb{Z}^x)$$

6.3. Computing Termination Sets. The following theorem is used to compute (overapproximations of) weakest non-termination preconditions from (overapproximations of) transition invariants.

Theorem 9. Let $P = \langle \mathbf{x}, Q, q_i, \Delta \rangle$ be a program, and let there be relations $R_{q,k}$, $1 \leq k \leq p_q$, for some $p_q \geq 1$, such that $\llbracket P \rrbracket^{TInv}(q, q) \subseteq \bigcup_{k=1}^{p_q} R_{q,k}$. Let

$$\mathcal{N} = \bigcup_{q \in Q} \left((\llbracket P \rrbracket^*(q_i, q))^{-1} \left(\bigcup_{k=1}^{p_q} \text{wnt}(R_{q,k}) \right) \right)$$

Then $\llbracket P \rrbracket^{wnt} \subseteq \mathcal{N}$. Moreover, if $\llbracket P \rrbracket^{TInv}(q, q) = \bigcup_{k=1}^{p_q} R_{q,k}$, then $\llbracket P \rrbracket^{wnt}(q_i) = \mathcal{N}$.

Proof. First suppose that $\llbracket P \rrbracket^{TInv}(q, q) = \bigcup_{k=1}^{p_q} R_{q,k}$ for all $q \in Q$.

“ \Rightarrow ” Let $\rho_1 = \langle q_i, \nu_0 \rangle \langle q_1, \nu_1 \rangle \langle q_2, \nu_2 \rangle \dots$ be an infinite run of P . Clearly, there exist infinitely many integers $1 \leq \ell_1 < \ell_2 < \ell_3 < \dots$ such that $q = q_{\ell_1} = q_{\ell_2} = q_{\ell_3} = \dots$ for some $q \in Q$. We construct an infinite meta-run $\rho_2 = \langle q_i, \nu_0 \rangle \langle q, \nu_{\ell_1} \rangle \langle q, \nu_{\ell_2} \rangle \dots$. It follows from definition of $\llbracket P \rrbracket^{TInv}$ that

$$(\nu_{\ell_j}, \nu_{\ell_{j+1}}) \in \llbracket P \rrbracket^{TInv}(q, q) = \llbracket P \rrbracket^{TInv}(q, q)$$

for all $j \geq 1$. We next rename valuations in ρ_2 to obtain $\rho_2 = \langle q_i, \mu_0 \rangle \langle q, \mu_1 \rangle \langle q, \mu_2 \rangle \dots$.

Let us assume that $\llbracket P \rrbracket^{TInv}(q, q) \Leftrightarrow \bigvee_{k=1}^p R_k$ for some $p \geq 1$. By definition of $\llbracket P \rrbracket^{TInv}$, it follows that for each $\ell > k \geq 1$, there exists $1 \leq j \leq p$ such that $(\mu_k, \mu_\ell) \in R_j$. Consequently, we can construct a function $f : \{(k, \ell) \mid \ell > k \geq 1\} \rightarrow \{R_1, \dots, R_p\}$ such that $(\mu_k, \mu_\ell) \in f(k, \ell)$ for all $\ell > k \geq 1$.

Let \sim be the kernel of f and thus, $(k, \ell) \sim (k', \ell')$ if and only if $f(k, \ell) = f(k', \ell')$. Clearly, \sim is an equivalence relation with finite index, since the range of f is finite. Consequently, by Ramsey theorem [30], there exists an infinite sequence of integers $1 \leq k_1 < k_2 < k_3 < \dots$ and an equivalence class $[(m, n)]_\sim$ for some m, n such that $(k, k_{i+1}) \sim (m, n)$ for all $i \geq 1$. Thus, there exists $1 \leq j \leq p$ such that $f(k, k_{i+1}) = R_j$ for all $i \geq 1$. Consequently, $\mu_{k_1} \mu_{k_2} \dots$ is an infinite run of R_j and hence, $\mu_{k_1} \in \text{wnt}(R_j)$. Since $(\mu_0, \mu_{k_1}) \in \llbracket P \rrbracket^*(q_i, q)$, by definition of $\llbracket P \rrbracket^*$, it follows that

$$\nu_0 = \mu_0 \in (\llbracket P \rrbracket^*(q_i, q))^{-1} (\text{wnt}(R_j)) \subseteq (\llbracket P \rrbracket^*(q_i, q))^{-1} \left(\bigcup_{k=1}^p \text{wnt}(R_k) \right) \subseteq \mathcal{N}$$

Thus, $\llbracket P \rrbracket^{wnt} \subseteq \mathcal{N}$.

“ \Leftarrow “ Clearly, $\bigcup_{k=1}^{p_q} \text{wnt}(R_{q,k})$ is the set of initial valuations of non-terminating runs that start in $q \in Q$, by definition of $\llbracket P \rrbracket^{TInv}$. Consequently, $(\llbracket P \rrbracket^*(q_i, q))^{-1} (\bigcup_{k=1}^{p_q} \text{wnt}(R_{q,k}))$ is the set of valuations in q_i from which a non-terminating run that loops infinitely at q exists. Consequently,

$$\mathcal{N} \stackrel{def}{=} \bigcup_{q \in Q} \left((\llbracket P \rrbracket^*(q_i, q))^{-1} \left(\bigcup_{k=1}^{p_q} \text{wnt}(R_{q,k}) \right) \right)$$

is the set of valuations in q_i from which a non-terminating run that loops in some $q \in Q$ exists and thus, $\mathcal{N} \subseteq \llbracket P \rrbracket^{wnt}$.

Next, observe that if $\llbracket P \rrbracket^{TInv}(q, q) \subseteq \bigcup_{k=1}^{p_q} R_{q,k}$ for all $q \in Q$, the “ \Rightarrow “ direction of the above proof still holds. \square

Next, we present an algorithm that computes an over-approximation of $\llbracket P \rrbracket^{wnt}$. We first compute an over-approximation of $\llbracket P \rrbracket^{TInv}$. To this end, we adapt the procedure summary algorithm from [10]. Then, an overapproximation of $\llbracket P \rrbracket^{wnt}$ can be computed by applying Theorem 9. Algorithm 2 achieves this by executing lines 4 and 5 for each control state $q \in Q$. Note that we can apply Algorithm 1 from Section 4.5 to compute the weakest non-termination set $\text{wnt}(R_j)$ at line 5.

Algorithm 2 Over-approximating the Weakest Non-termination Precondition of a Program

input A procedure $P = \langle \mathbf{x}, Q, q_i, \Delta \rangle$
output An over-approximation of $\llbracket P \rrbracket^{wnt}$
1: **function** WNT_APPROX($P = \langle \mathbf{x}, Q, q_i, \Delta \rangle$)
2: $\mathcal{N} \leftarrow \emptyset$
3: **for each** $q \in Q$ **do**
4: **let** $\llbracket P \rrbracket^{TInv}(q, q) \Rightarrow (R_1 \vee \dots \vee R_p)$ for some $R_1, \dots, R_p, p \geq 1$
5: $\mathcal{N} \leftarrow \mathcal{N} \vee (\llbracket P \rrbracket^*(q_i, q))^{-1} (\bigvee_{j=1}^p \text{WNT}(R_j))$
6: **return** \mathcal{N}

6.4. Flat Integer Programs. In this section, we define a class of integer programs for which our method computes precisely the weakest non-termination preconditions, as formulae in Presburger arithmetic. As a consequence, the universal termination problem is decidable for this class. A *flat integer program* is a program where:

- (1) each control state belongs to at most one cycle in the control flow graph (CFG)
- (2) for each cycle $q_1 \xrightarrow{R_1} q_2 \xrightarrow{R_2} \dots \xrightarrow{R_n} q_1$ in the CFG, the relation $(R_1 \circ \dots \circ R_n)$ is either octagonal or a finite monoid affine relation

Let P be a flat integer program. It is known that the reachability problem for flat integer programs is decidable [14, 23, 8] and that $\llbracket P \rrbracket^*$ can be effectively computed as a Presburger formula using e.g. a method from [10]. Consider Algorithm 3 that uses an auxiliary procedure $\text{LOOPLABEL}(P, q)$, which returns the composition of relations that label the unique cycle on which the control state q appears or empty relation if there is no such cycle. Let $q \in Q$ and let $L_q = \text{LOOPLABEL}(P, q)$. Since L_q is either an octagonal or finite monoid affine relation, the weakest non-termination set $\text{wnt}(L_q)$ is Presburger definable, as proved

in Sections 4 and 5. The weakest non-termination precondition can be computed by observing that, if the program has an infinite run, then this run will get stuck in some loop labeled L_q . Consequently, Algorithm 3 correctly returns a Presburger formula defining $\llbracket P \rrbracket^{wnt}$. The following theorem summarizes these observations.

Theorem 10. The weakest non-termination precondition of a flat integer programs is effectively computable and Presburger definable. Consequently, the termination problem is decidable for flat integer programs.

Algorithm 3 Weakest Non-termination Precondition for Flat Integer Programs

input A flat integer program $P = \langle \mathbf{x}, Q, q_i, \Delta \rangle$
output $\llbracket P \rrbracket^{wnt}$, the weakest non-termination set of P

- 1: **function** PROGRAMSUMMARY($P = \langle \mathbf{x}, Q, q_i, \Delta \rangle$)
- 2: $\mathcal{N} \leftarrow \emptyset$
- 3: **for each** $q \in Q$ **do**
- 4: $A \leftarrow \text{WNT}(\text{LOOPLABEL}(P, q))$
- 5: $\mathcal{N} \leftarrow \mathcal{N} \cup (\llbracket P \rrbracket^*(q_i, q))^{-1}(A)$
- 6: **return** \mathcal{N}

7. EXPERIMENTS

We have validated the methods described in this paper by automatically verifying termination of all the octagonal running examples, and of several integer programs synthesized from (i) programs with lists obtained using the translation scheme from [6] which generates an integer program from a program manipulating dynamically allocated single-selector linked lists, (ii) VHDL designs such as hardware counter and synchronous LIFO [31], (iii) small C programs with challenging loops and (iv) small recursive Java programs from [1] translated to non-recursive programs using the translation scheme from [3].

We have computed the weakest non-termination sets reported in Table 1 using the methods from Section 4 and 6 which we implemented in the FLATA tool [21]. By computing octagonal abstractions of disjuncts of a transition invariant, we have verified universal termination of the LISTCOUNTER and LISTREVERSAL programs. Next, we have verified the COUNTER and SYNLIPO programs by computing the precise transition invariant and then the weakest non-termination set, which was empty in both cases. Thus, these models have infinite runs for any input values, which is to be expected as they encode the behavior of synchronous reactive circuits. Similarly, we have computed the weakest non-termination preconditions for numerical programs ANUBHAV, COUSOT, LEQ, and PLUS.

Second, we have compared (Table 2) our method for termination of polynomially bounded linear affine loops from Section 5 with the examples given in [15], and found the same termination preconditions as they do, with one exception, in which we can prove universal termination in integer input values (row 3 of Table 2).

TABLE 1. Weakest Non-termination Sets for Integer Programs.

| Model | Size | | | Time [s] | Weakest Non-termination Set |
|----------------------------|---------|---------|--------------|----------|--------------------------------|
| | $\ x\ $ | $\ Q\ $ | $\ \Delta\ $ | | |
| (i) Examples from L2CA [6] | | | | | |
| listcounter | 4 | 31 | 35 | 1.2 | false |
| listreversal | 7 | 97 | 107 | 32.6 | false |
| (ii) VHDL models from [31] | | | | | |
| counter | 2 | 6 | 13 | 0.8 | true |
| register | 2 | 10 | 49 | 1.4 | true |
| synlifo | 3 | 43 | 1006 | 1016.4 | true |
| (iii) Examples from [22] | | | | | |
| anubhav | 29 | 20 | 25 | 3.2 | $i < 0$ |
| cousot | 29 | 31 | 34 | 4.0 | true |
| (iii) Examples from [1] | | | | | |
| leq | 3 | 5 | 6 | 0.6 | false |
| leq.modif | 3 | 5 | 6 | 2.4 | $x < 0 \wedge y < 0$ |
| plus | 3 | 7 | 9 | 0.7 | false |
| plus.modif | 3 | 7 | 9 | 0.9 | $x < 0 \vee y < 0$ |

TABLE 2. Termination preconditions for several program fragments from [15]

| PROGRAM | COOK ET AL. [15] | LINEAR AFFINE LOOPS |
|----------------------------------------------------------------------------------------------------------------|------------------------------------------------|---------------------------------------------------|
| if ($lvar \geq 0$) while ($lvar < 2^{30}$) $lvar = lvar \ll 1$; | $lvar > 0 \vee lvar < 0 \vee lvar \geq 2^{30}$ | $\neg(lvar=0) \vee lvar \geq 2^{30}$ |
| while ($x \geq N$) $x = -2*x + 10$; | $x > 5 \vee x + y \geq 0$ | $x \neq \frac{10}{3} \Leftrightarrow \text{true}$ |
| //@ requires $n > 200$ $x = 0$; while (1) if ($x < n$) { $x=x+y$; if ($x \geq 200$) break; } | $y > 0$ | $y > 0$ |

8. CONCLUSION

We have presented several methods for deciding conditional termination of several classes of program loops manipulating integer variables. The universal termination problem has been found to be decidable for octagonal relations and linear affine loops with the finite monoid property. For the class of polynomially bounded linear affine loops, we give sufficient termination conditions. Further, we extend the computation of weakest non-termination preconditions from simple loops to general programs, and define a class of programs, called flat, for which this computation yields precise results. Finally, we have implemented our method in the FLATA tool [21] and performed a number of preliminary experiments.

REFERENCES

- [1] Termination Competition 2011. <http://termcomp.uibk.ac.at/termcomp/home.seam>.
- [2] R. Alur and D. L. Dill. The theory of timed automata. In *proc. of REX Workshop*, volume 600 of *LNCS*, pages 45–73, Berlin, Heidelberg, 1991. Springer Verlag.
- [3] A. Podelski B. Cook and A. Rybalchenko. Summarization for termination: no return! *Formal Methods in System Design*, 35:369–387, 2009.

- [4] R. Bagnara, P. M. Hill, and E. Zaffanella. An improved tight closure algorithm for integer octagonal constraints. In *Proc. of VMCAI*, volume 4905 of *LNCS*, pages 8–21, Berlin, Heidelberg, 2008. Springer Verlag.
- [5] B. Boigelot. *Symbolic Methods for Exploring Infinite State Spaces*. PhD Thesis. Université de Liège, 1999.
- [6] A. Bouajjani, M. Bozga, P. Habermehl, R. Iosif, P. Moro, and T. Vojnar. Programs with lists are counter automata. In *Proc. of CAV*, volume 4144 of *LNCS*, pages 517–531, Berlin, Heidelberg, 2006. Springer Verlag.
- [7] M. Bozga, C. Gîrlea, and R. Iosif. Iterating octagons. In *Proc. of TACAS*, volume 5505 of *LNCS*, pages 337–351, Berlin, Heidelberg, 2009. Springer Verlag.
- [8] M. Bozga, R. Iosif, and F. Konečný. Fast acceleration of ultimately periodic relations. In *Proc. of CAV*, volume 6174 of *LNCS*, pages 227–242, Berlin, Heidelberg, 2010. Springer Verlag.
- [9] M. Bozga, R. Iosif, and F. Konečný. Deciding conditional termination. In *Proc. of TACAS*, volume 7214 of *LNCS*, pages 252–266, Berlin, Heidelberg, 2012. Springer Verlag.
- [10] M. Bozga, R. Iosif, and F. Konečný. Relational analysis of integer programs. Technical Report TR-2012-10, Verimag, Grenoble, France, 2012.
- [11] M. Bozga, R. Iosif, and Y. Lakhnech. Flat parametric counter automata. *Fundamenta Informaticae*, 91(2):275–303, 2009.
- [12] A. R. Bradley, Z. Manna, and H. B. Sipma. Linear ranking with reachability. In *Proc. of CAV*, volume 3576 of *LNCS*, pages 491–504, Berlin, Heidelberg, 2005. Springer Verlag.
- [13] M. Braverman. Termination of integer linear programs. In *Proc. of CAV*, volume 4144 of *LNCS*, pages 372–385, Berlin, Heidelberg, 2006. Springer Verlag.
- [14] H. Comon and Y. Jurski. Multiple counters automata, safety analysis and presburger arithmetic. In *Proc. of CAV*, volume 1427 of *LNCS*, pages 268–279, Berlin, Heidelberg, 1998. Springer Verlag.
- [15] B. Cook, S. Gulwani, T. Lev-Ami, A. Rybalchenko, and M. Sagiv. Proving conditional termination. In *Proc. of CAV*, volume 5123 of *LNCS*, pages 328–340, Berlin, Heidelberg, 2008. Springer Verlag.
- [16] T. H. Cormen, C. Stein, R. L. Rivest, and C. E. Leiserson. *Introduction to Algorithms*. McGraw-Hill Higher Education, 2nd edition, 2001.
- [17] G. Everest. *Recurrence sequences*. American Mathematical Soc., 2003.
- [18] A. Finkel and J. Leroux. How to compose presburger-accelerations: Applications to broadcast protocols. In *Proc. of FST TCS*, volume 2556 of *LNCS*, pages 145–156, Berlin, Heidelberg, 2002. Springer Verlag.
- [19] A. Gupta, T. A. Henzinger, R. Majumdar, A. Rybalchenko, and R. Xu. Proving non-termination. In *Proc. of POPL*, pages 147–158, New York, NY, USA, 2008. ACM.
- [20] V. Halava, T. Harju, M. Hirvensalo, and J. Karhumäki. Skolem’s problem – on the border between decidability and undecidability, 2005.
- [21] H. Hojjat, R. Iosif, F. Garnier, F. Konečný, V. Kuncak, and P. Rümmer. A verification toolkit for numerical transition systems. In *Proc. of FM*, 2012. To appear.
- [22] R. Jhala and K. L. McMillan. A practical and complete approach to predicate refinement. In *Proc. of TACAS*, volume 3920 of *LNCS*, pages 459–473, Berlin, Heidelberg, 2006. Springer Verlag.
- [23] J. Leroux and G. Sutre. Flat counter automata almost everywhere! In *Proc. of ATVA*, volume 3707 of *LNCS*, pages 489–503, Berlin, Heidelberg, 2005. Springer Verlag.
- [24] A. Mandel and I. Simon. On finite semigroups of matrices. *Theoretical Computer Science*, 5(2):101–111, 1977.
- [25] Z. Manna and A. Pnueli. *Temporal Verification of Reactive Systems: Safety*. Springer Verlag, 1995.
- [26] A. Miné. The octagon abstract domain. *Higher-Order and Symbolic Computation*, 19(1):31–100, 2006.
- [27] A. Podelski and A. Rybalchenko. A complete method for the synthesis of linear ranking functions. In *Proc. of VMCAI*, volume 2937 of *LNCS*, pages 465–486, Berlin, Heidelberg, 2004. Springer Verlag.
- [28] A. Podelski and A. Rybalchenko. Transition invariants. In *LICS’04*, pages 32–41, 2004.
- [29] M. Presburger. Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt. *Comptes rendus du I Congrès des Pays Slaves*, page 92–101, 1929.
- [30] F. P. Ramsey. On a problem of formal logic. *Proc. of the London Mathematical Society*, 30:264–285, 1930.
- [31] A. Smrcka and T. Vojnar. Verifying parametrised hardware designs via counter automata. In *Proc. of HVC*, volume 4899 of *LNCS*, pages 51–68, Berlin, Heidelberg, 2007. Springer Verlag.

- [32] K. Sohn and A. Van Gelder. Termination detection in logic programs using argument sizes. In *Proc. of PODS*, pages 216–226, New York, NY, USA, 1991. ACM.
- [33] A. Tiwari. Termination of linear programs. In *Proc. of CAV*, volume 3114 of *LNCS*, pages 70–82, Berlin, Heidelberg, 2004. Springer Verlag.
- [34] A. M. Turing. On computable numbers, with an application to the entscheidungsproblem. *Proceedings of the London Mathematical Society*, 42:230–265, 1936.